

Northeastern University

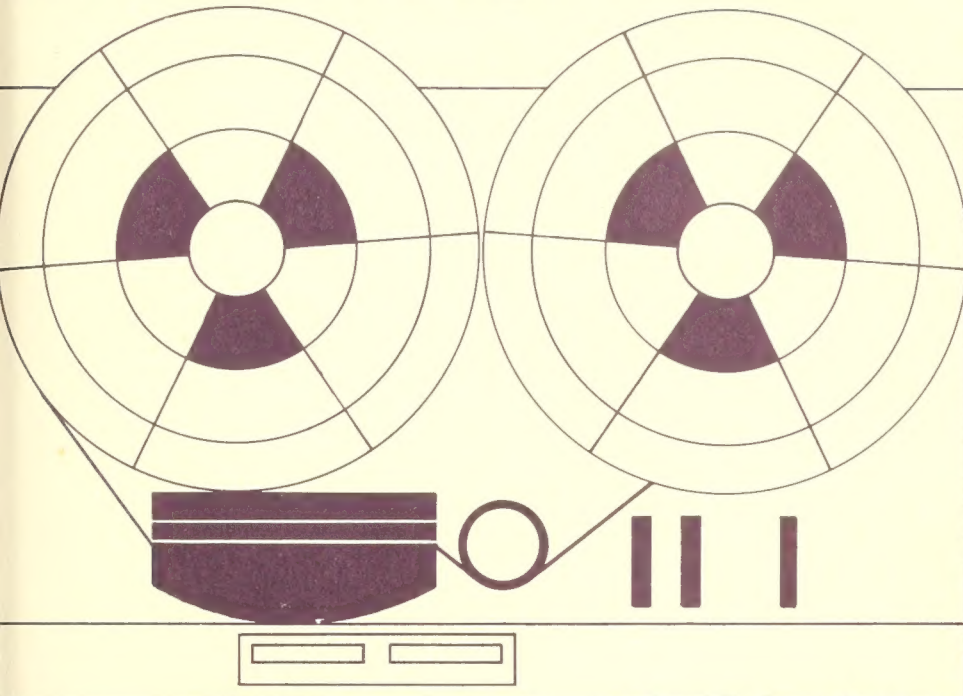


**School of Law
Library**

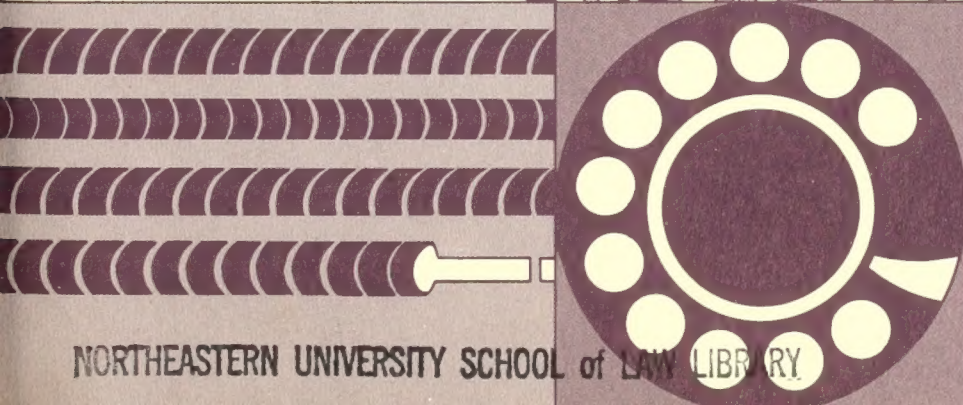
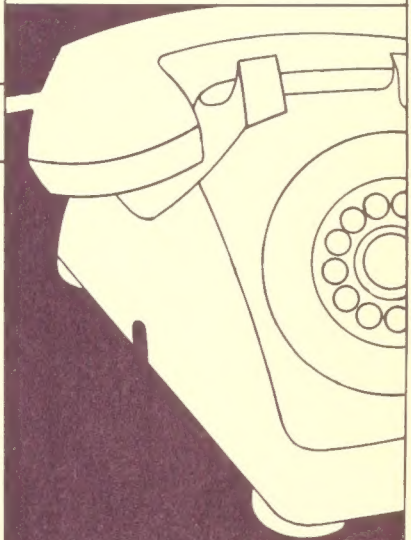


Commission Hearings

Volume 2



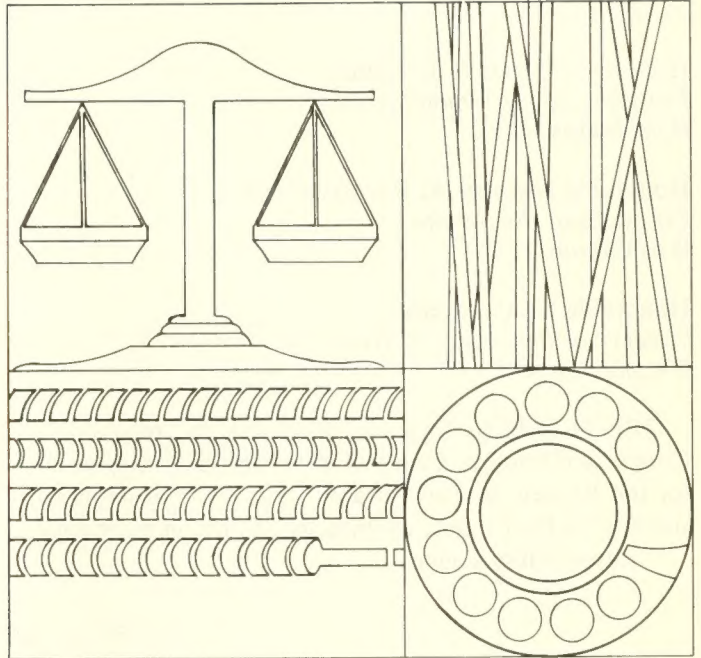
NATIONAL
COMMISSION
FOR THE REVIEW
OF FEDERAL
AND STATE LAWS
RELATING TO
WIRETAPPING AND
ELECTRONIC
SURVEILLANCE



RECEIVED

DEC 10 1976

N. U. LAW LIBRARY



Commission Hearings Volume 2

Supporting
Materials
for the Report
of the

**NATIONAL
COMMISSION
FOR THE REVIEW
OF FEDERAL
AND STATE LAWS
RELATING TO
WIRETAPPING AND
ELECTRONIC
SURVEILLANCE
WASHINGTON:
1976**

Y3.W74/2:2H35/v.2

May be cited as
NWC Commission Hearings,
Vol. 2

**NATIONAL COMMISSION FOR THE REVIEW OF FEDERAL AND STATE LAWS
RELATING TO WIRETAPPING AND ELECTRONIC SURVEILLANCE**

1875 Connecticut Avenue, N.W.
Washington, D.C. 20009

April 30, 1976

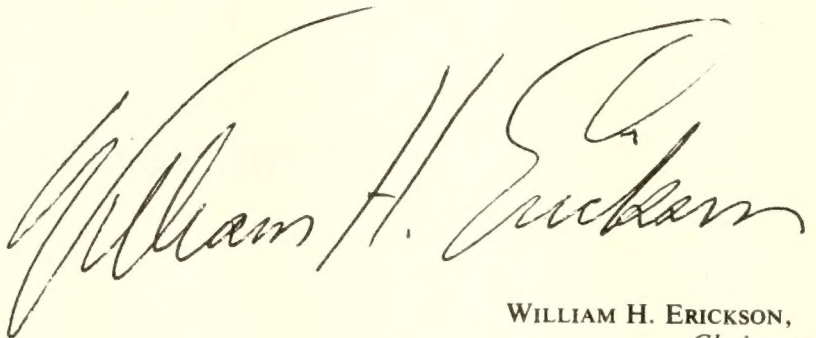
Honorable GERALD R. FORD,
President of the United States,
Washington, D.C.

Honorable NELSON A. ROCKEFELLER,
President of the Senate,
Washington, D.C.

Honorable CARL ALBERT,
Speaker of the House of Representatives,
Washington, D.C.

GENTLEMEN: In accordance with the provisions of section 804 of Public Law No. 351, Ninetieth Congress (Omnibus Crime Control and Safe Streets Act of 1968), as amended, the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance herewith submits its final report of findings and recommendations.

Respectfully yours,



WILLIAM H. ERICKSON,
Chairman.

Library of Congress Card No. 75-619445

5155100

NATIONAL COMMISSION FOR THE REVIEW OF FEDERAL AND STATE LAWS RELATING TO WIRETAPPING AND ELECTRONIC SURVEILLANCE

APPOINTED BY THE PRESIDENT:

Chairman:

William H. Erickson, Associate Justice of the
Supreme Court of Colorado

Members:

Richard R. Andersen, Chief of Police, Omaha,
Nebraska

G. Robert Blakey, Professor of Law, Cornell
University Law School

Hon. Samuel R. Pierce, Jr., Attorney, New York
City

Frank J. Remington, Professor of Law, University
of Wisconsin Law School

Hon. Florence P. Shientag, Attorney, New York
City

Alan F. Westin, Professor of Public Law and
Government, Columbia University

APPOINTED BY THE PRESIDENT OF THE SENATE:

Senator John L. McClellan

Senator Roman L. Hruska

Senator Robert Taft, Jr.

Senator James Abourezk

APPOINTED BY THE SPEAKER OF THE HOUSE OF REPRESENTATIVES:

Congressman Robert W. Kastenmeier

Congressman Thomas F. Railsback

Congressman John F. Seiberling*

Congressman M. Caldwell Butler**

*Appointed March 1975 to replace Congressman Don Edwards,
a member during the 93d Congress.

**Appointed March 1975 to replace Congressman Sam Steiger,
a member during the 93d Congress.

COMMISSION STAFF

Executive Director

Kenneth J. Hodson

Counsel for State Laws Study

Milton M. Stein

Counsel for Federal Laws Study

David J. Cook

Chief Investigator

Michael J. Hershman

Research Adviser

Margery J. Elfin

Staff Attorneys

Glenn M. Feldman

Edward J. Gallagher

Michael L. Lipman

Hal B. Patterson

Legal Research

Stephen O. Allaire

Sandra L. Thomas

Social Research

John H. Maberry

Marilyn Mode

Ellen A. Patterson

Assistant Investigator

John J. Creighton

Administrative

Mildred F. Dolan

Jacqueline I. Hallowell

Donald B. Harper

Secretarial

Suzanne Charlick

Muriel A. DeMarne

Fann D. Harvey

Wanda G. Henderson

Elaine E. Holloman

Elizabeth L. McCulley

Jean C. Teuteberg

CONSULTANTS AND ADVISERS

Investigative Attorneys

Tobias Berman, New York City
Gary L. Gardner, Northville, N. Y.
Randolph N. Jonakait, New York City
Thomas A. Kennelly, Washington, D. C.
Jack Lipson, New York City
Geoffrey W. Peters, Professor of Law, Creighton University, Omaha, Nebr.

National Security Consultant

Dr. John T. Elliff, Associate Professor of Politics, Brandeis University, Waltham, Mass.

Comparative Law Consultant

H. H. A. Cooper, Director, Criminal Law Education and Research Center, New York University School of Law

Consulting Attorneys

William I. Aronwald, Chief, Federal Strike Force, New York City
William M. Lenck, Drug Enforcement Administration, Washington, D. C.
James L. Lyons, Washington, D. C.
Peter R. Richards, Deputy Attorney General, State of New Jersey
Frank J. Rogers, Special Prosecutor, Narcotics, New York City
Herman Schwartz, Professor of Law, State University of New York, Buffalo
Peter F. Vaira, Chief, Federal Strike Force, Chicago, Illinois
Roger E. Zuckerman, Washington, D. C.

Scientific Consultants

William E. Harward, Chief, Radio Engineering Section, FBI
Dr. Michael H. L. Hecker, Stanford Research Institute, Palo Alto, California
Dr. Paul Tamarkin, Riverside Research Corp., Arlington, Va.

Carmen J. Tona, Chief Electronics Engineer for Law Enforcement, CALSPAN Corp., Buffalo, N. Y.

John S. VanDewerker, Manager, Systems Division, Ashby & Associates, Washington, D. C.

Mark R. Weiss, Professor, Computer Science, Queens College, City University of New York

John P. Wilgus, Assistant Chief, Radio Engineering Section, FBI

Field Investigators

James T. Fahy, Retired Detective First Class, New York City Police Department

William W. Turner, Author, Private Investigator (former FBI agent)

Writing and Editing

James G. Carr, Professor of Law, Toledo University, School of Law, Toledo, Ohio

Jeffrey D. Stansbury, Writer

Joseph Foote, Editorial Adviser

Editing and Proofreading:

Editorial Experts, Laura Horowitz, Director, Springfield, Va.

Law Enforcement Advisers

James Adams, Assistant to Director, FBI

Capt. Clayton R. Anderson, Chief, Intelligence Bureau, District Attorney's Office, Los Angeles, Calif.

Dr. Don R. Harris, CACI, Inc., Arlington, Va.

Walter LaPrade, Special Agent in Charge, FBI, Newark, N.J.

John A. Lelwica, Special Agent, FBI, Newark, N.J.

William P. McCarthy, Retired Deputy Police Commissioner, New York City

Fred J. Rayano, Principal Investigator, Office of New York State Special Prosecutor

Phil Smith, Domestic Intelligence, Drug Enforcement Administration

Alvin A. Staffeld, Inspector, FBI

NATIONAL COMMISSION FOR THE REVIEW OF FEDERAL AND STATE LAWS RELATING TO WIRETAPPING AND ELECTRONIC SURVEILLANCE

ENABLING ACT

Sec. 804 of Pub. L. 90-351, June 19, 1968, as amended by Pub. L. 91-644, Pub. L. 93-609, and Pub. L. 94-176 provided:

"(a) [ESTABLISHMENT] There is hereby established a National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance (hereinafter in this section referred to as the 'Commission').

"(b) [MEMBERSHIP] The Commission shall be composed of fifteen members appointed as follows:

"(A) Four appointed by the President of the Senate from Members of the Senate;

"(B) Four appointed by the Speaker of the House of Representatives from Members of the House of Representatives; and

"(C) Seven appointed by the President of the United States from all segments of life in the United States including lawyers, teachers, artists, businessmen, newspapermen, jurists, policemen, and community leaders, none of whom shall be officers of the executive branch of the Government.

"(c) [CHAIRMAN; VACANCIES] The President of the United States shall designate a Chairman from among the members of the Commission. Any vacancy in the Commission shall not affect its powers but shall be filled in the same manner in which the original appointment was made.

"(d) [FUNCTION] It shall be the duty of the Commission to conduct a comprehensive study and review of the operation of the provisions of this title, in effect on the effective date of this section, to determine the effectiveness of such provisions during the six-year period immediately following the date of their enactment.

"(e) [PERSONNEL; APPOINTMENT, COMPENSATION AND QUALIFICATIONS] (1) Subject to such rules and regulations as may be adopted by the Commission, the Chairman shall have the power to—

"(A) appoint and fix the compensation of an Executive Director, and such additional staff personnel as he deems necessary, without regard to the provisions of title 5, United States Code, governing appointments in the competitive service, and without regard to the provisions of chapter 51 and subchapter III of chapter 53 of such title relating to classification and General Schedule pay rates, but at rates not in excess of the maximum rate for GS-18 of the General Schedule under section 5332 of such title; and

"(B) procure temporary and intermittent services to the same extent as is authorized by section 3109 of title 5, United States Code, but at rates not to exceed \$100 a day for individuals.

"(2) In making appointments pursuant to paragraph (1) of this subsection, the Chairman shall include among his appointment individuals determined by the Chairman to be competent social scientists, lawyers, and law enforcement officers.

"(f) [COMPENSATION, TRAVEL AND OTHER EXPENSES] (1) A member of the Commission who is a Member of Congress shall serve without additional compensation, but shall be reimbursed for travel, subsistence, and other necessary expenses incurred in the performance of duties vested in the Commission.

"(2) A member of the Commission from private life shall receive \$100 per diem when engaged in the actual performance of duties vested in the Commission, plus reimbursement for travel, subsistence, and other necessary expenses incurred in the

performance of such duties.

"(g)(1) Notwithstanding section 2515 of title 18, United States Code, the Commission or any duly authorized subcommittee or member thereof may, for the purpose of carrying out the provisions of this title, hold such hearings, sit and act at such times and places, administer such oaths, and require by subpoena or otherwise the attendance testimony of such witnesses and the production of such books, records, correspondence, memorandums, papers and documents as the Commission or such subcommittee or member may deem advisable. Any member of the Commission may administer oaths or affirmations to witnesses appearing before the Commission or before such subcommittee or member. Subpenas may be issued under the signature of the Chairman or any duly designated member of the Commission, and may be served by any person designated by the Chairman or such member.

"(2) In the case of contumacy or refusal to obey a subpoena issued under subsection (1) by any person who resides, is found, or transacts business within the jurisdiction of any district court of the United States, the district court, at the request of the Chairman of the Commission, shall have jurisdiction to issue to such person an order requiring such person to appear before the Commission or a subcommittee or member thereof, there to produce evidence if so ordered, or there to give testimony touching the matter under inquiry. Any failure of any such person to obey any such order of the court may be punished by the court as a contempt thereof.

"(3) The Commission shall be 'an agency of the United States' under subsection (1), section 6001, title 18, United States Code for the purpose of granting immunity to witnesses.

"(4) Each department, agency, and instrumentality of the executive branch of the Government, including independent agencies, is authorized and directed to furnish to the Commission, upon request made by the Chairman, on a reimbursable basis or otherwise, such statistical data, reports, and other information as the Commission deems necessary to carry out its functions under this title. The Chairman is further authorized to call upon the departments, agencies, and other offices of the several States, to furnish, on a reimbursable basis or otherwise, such statistical data, reports, and other information as the Commission deems necessary to carry out its functions under this title.

"(5) Whenever the Commission or any subcommittee determines by majority vote to meet in a closed session, sections 10(a)(1) and (3) and 10(b) of the Federal Advisory Committee Act (86 Stat. 770; 5 U.S.C. Appendix) shall not apply with respect to such meeting, and section 552 of title 5, United States Code, shall not apply to the records, reports, and transcripts of any such meeting.

"(h) [REPORTS TO PRESIDENT AND CONGRESS; TERMINATION DATE] The Commission shall make such interim reports as it deems advisable, and it shall make a final report of its findings and recommendations to the President of the United States and to the Congress on or before April 30, 1976. Sixty days after submission of its final report, the Commission shall cease to exist.

"(i) [CONFLICT OF INTEREST; EXEMPTION] (1) Except as provided in paragraph (2) of this subsection, any member of the Commission is exempted, with respect to his appointment, from the operation of sections 203, 205, 207, and 209 of title 18, United States Code.

"(2) The exemption granted by paragraph (1) of this subsection

tion shall not extend—

“(A) to the receipt of payment of salary in connection with the appointee’s Government service from any source other than the private employer of the appointee at the time of his appointment, or

“(B) during the period of such appointment, to the prosecution, by any person so appointed, of any claim against the Government involving any matter with which such person, during such period, is or was directly connected by reason of such appointment.

“(j) [APPROPRIATIONS] There is authorized to be appropriated such sum as may be necessary to carry out the provisions of this section.

“(k) [EFFECTIVE DATE] The foregoing provisions of this section shall take effect upon the expiration of the fifth year period

immediately following the date of the enactment of this Act [June 19, 1968].”

[New: Added by Pub. L. 93-609. Jan. 2, 1975]

For purposes of section 108 of title 1, United States Code, section 20(c) of the Omnibus Crime Control Act of 1970 shall be deemed to provide expressly for the revival of section 804 of the Omnibus Crime Control and Safe Streets Act of 1968.

REPEAL

Sec. 1212 of the Act of Oct. 15, 1970, Pub. L. 91-452, repealed sec. 804 of the Act of June 19, 1968, Pub. L. 90-351.

However, section 20 of the Act of Jan. 2, 1971, Pub. L. 91-644, repealed Sec. 1212 of Pub. L. 91-452 and contained certain amendments to section 804 of Pub. L. 90-351, which are set out above.

SCOPE OF THE COMMISSION INQUIRY

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 authorized court-ordered wiretapping and electronic surveillance (hereinafter "wiretapping") by Federal and State authorities. In Section 804 of Title III, Congress also provided that a National Commission would come into existence some six years later to review the operation of the wiretap Act.

This Commission was designated the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance. Its enabling statute brought it into existence on June 19, 1973, but because of a delay in the appointment of the seven public members and the four members from the House of Representatives, the Commission was unable to commence its work until April 1974. The Commission is charged with making its final report to the President and the Congress by April 30, 1976.

Congress charged the Commission with determining whether wiretapping and electronic surveillance under the Act is an effective tool in law enforcement, whether wiretapping under the Act properly protects the privacy of the individual, and whether the Act is effective in preventing illegal wiretapping. The Commission went about its work of gathering evidence to permit it to make an objective assessment of wiretapping in four basic ways, outlined as follows:

(1) *Law Enforcement Effectiveness Conference.* At an early stage of its work, the Commission was confronted with the problem of developing a standard by which it could measure the effectiveness of wiretapping in law enforcement. Research disclosed that no law enforcement agency had published formal guidelines or instructional courses that would be useful in determining what kinds of cases could (best) (only) be solved by the use of wiretapping. In August 1974, fourteen experienced prosecutors and law enforcement officers from Federal, State, and local agencies met with members of the Commission staff and several Commission members for a three-day, free-wheeling, seminar-type conference, designed to elicit information about the proper and improper use of wiretapping in law enforcement. Commissioner G. Robert Blakey moderated the sessions. The transcript of these sessions appears as a separate volume of the supporting materials for the Commission Report, under the title *Law Enforcement Effectiveness Conference*.

(2) *Staff Studies and Surveys.* Members of the Commission staff, aided by parttime advisers and consultants in the field, visited 46 separate State and local prosecutorial jurisdictions (one additional

jurisdiction was interviewed by telephone) and 12 Federal geographical jurisdictions for the purpose of interviewing knowledgeable prosecutors, defense counsel, judges, police, and criminal investigators. A random sampling of cases in which wiretapping or electronic surveillance was used was studied with a view to determining the effectiveness of these techniques. Particular consideration was given to determining whether wiretapping enabled law enforcement officers to penetrate higher in a criminal hierarchy than would have been possible had this technique not been used. Four of the states visited did not have a state law permitting law enforcement to use court-ordered wiretapping, although these states were deemed to have a significant organized crime problem. An attempt was made to compare the effectiveness of law enforcement against organized crime in states which have court-ordered wiretapping with states which do not permit court-ordered wiretapping.

A separate report was prepared for each jurisdiction visited, including, when appropriate, a summary of each case analyzed. These reports are combined, with the results of two mail surveys of specialized monitoring problems, into a separate volume of the supporting materials for the Commission Report, under the title *Staff Studies and Surveys*.

(3) *Commission Studies.* As a means of providing the Commission members with background information concerning various aspects of wiretapping, a number of studies were prepared. These studies appear in a separate volume of the papers supporting the Commission Report, under the title *Commission Studies*. The titles of the separate studies are as follows:

- (a) State of the Law of Electronic Surveillance
- (b) Strategy and Tactics in the Prosecution and Defense of Complex Wire-Interception Cases
- (c) Comparative Law Aspects of Wiretapping and Electronic Surveillance
- (d) State of the Art of Electronic Surveillance
- (e) The Authentication of Magnetic Tapes: Current Problems and Possible Solutions

(4) *Commission Hearings.* To provide the maximum public exposure for its proceedings, most of the evidence considered by the Commission was presented under oath by some 100 witnesses during seventeen days of public hearings at Washington, D.C. The witnesses included knowledgeable persons in all fields related to wiretapping and electronic surveillance. These hearings were transcribed and published in two separate volumes of the supporting materials for the Commission Report, under the title *Commission Hearings*.

LIST OF SUPPORTING MATERIALS

LAW ENFORCEMENT EFFECTIVENESS CONFERENCE

STAFF STUDIES AND SURVEYS

- Survey of Electronic Surveillance under State Law: Jurisdictional Reports
- Survey of Electronic Surveillance under Federal Law: Jurisdictional Reports
- Legal Ethics of Consensual Monitoring and Advantages and Disadvantages of Service Quality Monitoring

COMMISSION STUDIES

- State of the Law of Electronic Surveillance
Commission Staff
- Strategy and Tactics in the Prosecution and Defense of Complex Wire-Interception Cases
Roger E. Zuckerman and James L. Lyons
- Comparative Law Aspects of Wiretapping and Electronic Surveillance
H.H.A. Cooper
- State of the Art of Electronic Surveillance
John S. VanDewerker of Ashby & Associates
- The Authentication of Magnetic Tapes: Current Problems and Possible Solutions
Mark R. Weiss and Michael H. L. Hecker

COMMISSION HEARINGS

VOLUME I

Hearing Days and Witnesses

September 16, 1974

- William B. Saxbe, United States Attorney General
- Henry E. Petersen, Assistant Attorney General, Criminal Division, U.S. Department of Justice
- William S. Lynch, Chief, Organized Crime and Racketeering Section, U.S. Department of Justice
- John R. Bartels, Jr., Administrator, Drug Enforcement Administration

September 17, 1974

- Clarence M. Kelley, Director, Federal Bureau of Investigation
- James Adams, Assistant to the Director in Charge of Investigations, Federal Bureau of Investigation
- William Cleveland, Assistant Director in Charge of Special Investigations, Organized Crime Division, Federal Bureau of Investigation
- John Kelly, Supervisor in Charge of Special Investigations, Organized Crime Division, Federal Bureau of Investigation

December 2, 1974

(Meeting adjourned because of lack of quorum.)

December 3, 1974

- David R. Macdonald, Assistant Secretary of Enforcement, Operations and Tariff Affairs, U.S. Department of the Treasury
- Billy E. Modesitt, Special Agent, Drug Enforcement Administration, Detroit, Michigan; former U.S. Customs Agent
- Atlee W. Wampler, III, Attorney-in-Charge, Miami Organized Crime Strike Force, U.S. Department of Justice

March 18, 1975

- Arlen Specter, former District Attorney, Philadelphia, Pennsylvania
- Mario Merola, District Attorney, Bronx County, New York
- Joseph Lordi, County Prosecutor, Essex County (Newark), New Jersey
- Jack Lazarus, District Attorney, Monroe County (Rochester), New York
- Pierre Leval, First Assistant District Attorney, New York County, New York
- John Breslin, Chief, Rackets Bureau, Bronx County District Attorney's Office, Bronx, New York
- Ronald Goldstock, Deputy Chief, Rackets Bureau, Bronx County District Attorney's Office, Bronx, New York
- Peter Grishman, Chief, Narcotics Bureau, Bronx County District Attorney's Office, Bronx, New York
- R. Michael Haynes, Assistant to the Special Prosecutor for Narcotics, New York City
- John Matthews, III, Director, City-County Strike Force, Essex County Prosecutor's Office, Newark, New Jersey
- Vincent Mitrano, First Assistant District Attorney, Monroe County, New York

March 19, 1975

- William Hyland, Attorney General of the State of New Jersey
- Peter Richards, Associate Director, Organized Crime and Special Prosecutions Section, Attorney General's Office, New Jersey
- Arnold Markle, District Attorney, New Haven County, Connecticut
- Joseph Phillips, Chief Assistant to the Special Prosecutor for Corruption, New York
- Neil O'Brien, Executive Assistant District Attorney, Queens County, New York
- Larry Finnegan, Chief, Investigations Bureau, Queens County District Attorney's Office, Queens, New York

David Cunningham, Chief, Trial Section, Office of the Special Prosecutor for Narcotics, New York

Barry Friedman, Chief, Rackets Bureau, Kings County District Attorney's Office, Brooklyn, New York

March 20, 1975

Ronald Goldstock, Deputy Chief, Rackets Bureau, Bronx County District Attorney's Office, Bronx, New York

William Aronwald, Attorney-in-Charge, Manhattan Organized Crime Strike Force, U.S. Department of Justice

Robert Nicholson, Detective Sergeant, New York City Police Department, New York County District Attorneys Squad, New York, New York

Richard Tammamo, Special Agent, Federal Bureau of Investigation, New York City Division

April 9, 1975

(Commission business meeting; no witnesses.)

April 22, 1975

Hon. Charles W. Joiner, U.S. District Court Judge, Eastern District of Michigan, Detroit, Michigan

Hon. John F. Dooling, Jr., U.S. District Court Judge, Eastern District of New York, Brooklyn, New York

Hon. Milton Mollen, Justice of the Supreme Court of the State of New York, Kings County, New York

Hon. Joseph Sullivan, Justice of the Supreme Court of the State of New York, Bronx County, New York

Hon. Henry J. Naruk, Judge, Superior Court of Connecticut, Middletown, Connecticut

Neil Fink, Esq., Defense Attorney, Detroit, Michigan

Stanley Arkin, Esq., Defense Attorney, New York, New York

April 23, 1975

James K. O'Malley, Defense Attorney, Pittsburgh, Pennsylvania

James Hogan, Esq., Defense Attorney, Miami Beach, Florida

William P. McCarthy, former Deputy Police Commissioner of New York City

Ronald G. Martin, Investigator, New York State Police

James Foody, Lieutenant, New York State Police

Richard Bolton, Counsel, New York State Police

Donald Brandon, Assistant Deputy Superintendent, Bureau of Criminal Investigations, New York State Police

Evan Miles, Captain and Chief Investigator, City-County Strike Force, Essex County Prosecutor's Office, Newark, New Jersey

Steven Bertucelli, Captain and Commanding Officer, Organized Crime Bureau, Dade County Office of Public Safety, Miami, Florida

Earl Campbell, Legal Officer, Phoenix Police Department, Phoenix, Arizona

May 19, 1975

Theodore L. Vernier, Regional Director, Drug Enforcement Administration, Detroit, Michigan

John G. Evans, Special Agent in Charge, Drug Enforcement Administration, Atlanta, Georgia

Alwin C. Coward, Special Agent, Drug Enforcement Administration, Miami, Florida

Gary G. Worden, Section Chief, Technical Operations Division, Drug Enforcement Administration, Washington, D.C.

Albert W. Seeley, Chief, Special Investigations Branch, United States Customs Service, Washington, D.C.

Laurence Leff, Executive Assistant, Nassau County District Attorney's Office, Nassau County, New York

VOLUME 2

Hearing Days and Witnesses

May 20, 1975

William V. Cleveland, Assistant Director in Charge of Special Investigations, Organized Crime Division, Federal Bureau of Investigation, Washington, D.C.

John R. Barron, Supervisor, Criminal Intelligence Squad, Federal Bureau of Investigation, Los Angeles, California

Robert G. Sweeney, Supervisor, Organized Crime Division, Federal Bureau of Investigation, New York, New York

Benjamin P. Grogan, Supervisor, Organized Crime Division, Federal Bureau of Investigation, Miami, Florida

James C. Esposito, Assistant Supervisor, Organized Crime Division, Federal Bureau of Investigation, Detroit, Michigan

May 21, 1975

Edward T. Joyce, Deputy Chief, Organized Crime and Racketeering Section, U.S. Justice Department, Washington, D.C.

Peter Schlamm, Assistant United States Attorney, Brooklyn, New York

Thomas E. Kotoske, Attorney-in-Charge, San Francisco Organized Crime Strike Force, U.S. Department of Justice

June 9, 1975

Joseph Busch, District Attorney, Los Angeles County, California

Kenneth Gillis, Chief, Special Prosecutions Bureau, Cook County State's Attorney's Office, Chicago, Illinois

Daniel McFadden, Lieutenant, Organized Crime Unit, Philadelphia Police Department, Philadelphia, Pennsylvania

Nicholas Iavarone, Chief, Organized Crime and Corruption Task Force, Cook County State's Attorney's Office, Chicago, Illinois

James R. Thompson, Jr., United States Attorney, Northern District of Illinois

Walter M. Phillips, Jr., Special Prosecutor for Corruption, Philadelphia, Pennsylvania

June 10, 1975

Hon. Herbert Stern, U.S. District Court Judge, District of New Jersey

Ramsey Clark, former Attorney General of the United States

R. Kent Greenawalt, Professor, Columbia University School of Law

Richard Uviller, Professor, Columbia University School of Law

June 11, 1975

Edith Lapidus, Professor, Queens College, New York

Herman Schwartz, Professor, State University of New York at Buffalo, School of Law

June 25, 1975

Jack N. Holcomb, President, Audio Intelligence Devices, Inc.

A. T. Bower, Manager, Government Sales, Bell & Howell Communications Co.

Michael J. Morrissey, formerly of B.R. Fox Company, Inc.

John S. VanDewerker, General Manager, Systems Division, Ashby & Associates

James T. Fahy, Consultant, National Wiretap

Commission

Carroll M. Lynn, Chief of Police, Houston, Texas

Anthony J.P. Farris, former U.S. Attorney, Southern District of Texas

Joseph Jaffe, Assistant United States Attorney, Southern District of New York

Jerris E. Bragan, former private investigator

June 26, 1975

Allen E. Ertel, District Attorney, Williamsport, Pennsylvania

Jerry N. Schneider, President, Jerry Schneider & Company

Richard L. Coulter, Corporate Security Director, Hewlett Packard Co.

Allen Bell, President, Dektor Counterintelligence and Security, Inc.

Martin L. Kaiser, President, Martin L. Kaiser, Inc.

Ben Jamil, Communications Control Corporation

John S. VanDewerker, General Manager, Systems Division, Ashby & Associates

Milo A. Speriglio, Director and Chief, Nick Harris Detectives, Inc.

H. Philip Nesbitt, Assistant Director of Investigations, Pinkerton's, Inc.

Samuel W. Daskam, General Manager, F.G. Mason Engineering, Inc.

June 27, 1975

James Reynolds, Attorney, Criminal Division, U.S. Department of Justice

William Caming, Attorney, American Telephone and Telegraph

John P. Linehan, Professor, Seminole Junior College

Neil Beller, Division Attorney, Central Telephone Company of Nevada

Michael Simon, Special Agent, Federal Bureau of Investigation, Las Vegas, Nevada

Karl Berolzheimer, General Counsel for Central Telephone & Utilities Corporation

CONTENTS

Alphabetic List of Witnesses

	Page
Adams, James, Assistant to the Director in Charge of Investigations, Federal Bureau of Investigation.....	93
Arkin, Stanley, Esquire, Defense Attorney, New York, New York.....	607
Aronwald, William, Attorney-in-Charge, Manhattan Organized Crime Strike Force, U.S. Department of Justice	413
Bartels, John R., Jr., Administrator, Drug Enforcement Administration	82
Barron, John R. Supervisor, Criminal Intelligence Squad, Federal Bureau of Investigation, Los Angeles, California	862
Bell, Allen, President, Dektor Counterintelligence and Security, Inc.	1400
Beller, Neil, Division Attorney, Central Telephone Company of Nevada.....	1647
Berolzheimer, Karl, General Counsel for Central Telephone & Utilities Corporation.....	1647
Bertucelli, Steven, Captain and Commanding Officer, Organized Crime Bureau, Dade County Office of Public Safety, Miami, Florida.....	695
Bolton, Richard, Counsel, New York State Police	654
Bower, A. T., Manager, Government Sales, Bell & Howell Communications Company	1242
Bragan, Jerris E., former private investigator.....	1307
Brandon, Donald, Assistant Deputy Superintendent, Bureau of Criminal Investigations, New York State Police	654
Breslin, John, Chief, Rackets Bureau, Bronx County District Attorney's Office, Bronx, New York.....	335
Busch, Joseph, District Attorney, Los Angeles County, California	920
Caming, William, Attorney, American Telephone and Telegraph	1546
Campbell, Earl, Legal Officer, Phoenix Police Department, Phoenix, Arizona.....	705
Clark, Ramsey, Former Attorney General of the United States.....	1008
Cleveland, William V., Assistant Director in Charge of Special Investigations, Organized Crime Division, Federal Bureau of Investigation	835
Coulter, Richard L., Corporate Security Director, Hewlett-Packard Company.....	1371
Coward, Alwin C., Special Agent, Drug Enforcement Administration, Miami, Florida.....	737
Cunningham, David, Chief, Trial Section, Office of the Special Prosecutor for Narcotics, New York City.....	390
Daskam, Samuel W., General Manager, F. G. Mason Engineering, Inc.	1452
Dooling, Hon. John F., Jr., U.S. District Court Judge, Eastern District of New York, Brooklyn, New York...	540
Ertel, Allen E., District Attorney, Williamsport, Pennsylvania.....	1345
Esposito, James C., Assistant Supervisor, Organized Crime Division, Federal Bureau of Investigation, Detroit, Michigan.....	880
Evans, John G., Special Agent in Charge, Drug Enforcement Administration, Atlanta, Georgia	728
Fahy, James T., Consultant, National Wiretap Commission	1263
Farris, Anthony J. P., former U.S. Attorney, Southern District of Texas.....	1290
Fink, Neil, Esquire, Defense Attorney, Detroit, Michigan	598
Finnegan, Lawrence J., Chief, Investigations Bureau,	

Queens County District Attorney's Office,	
Queens, New York.....	390
Foody, James, Lieutenant, New York State Police	654
Friedman, Barry, Chief, Rackets Bureau, Kings County District Attorney's Office, Brooklyn, New York.....	390
Gillis, Kenneth, Chief, Special Prosecutions Bureau, Cook County State's Attorney's Office, Chicago, Illinois	936, 961
Goldstock, Ronald, Deputy Chief, Rackets Bureau, Bronx County District Attorney's Office, Bronx, New York	335, 413
Greenawalt, R. Kent, Professor, Columbia University School of Law	1030
Grishman, Peter, Chief, Narcotics Bureau, Bronx County District Attorney's Office, Bronx, New York.....	335
Grogan, Benjamin P., Supervisor, Organized Crime Division, Federal Bureau of Investigation, Miami, Florida.....	874
Haynes, R. Michael, Assistant to the Special Prosecutor for Narcotics, New York City	335, 382
Hogan, James, Esquire, Defense Attorney, Miami Beach, Florida.....	630
Holcomb, Jack N., President, Audio Intelligence Devices, Inc.	1243
Hyland, William, Attorney General of the State of New Jersey	353
Iavarone, Nicholas, Chief, Organized Crime and Corruption Task Force, Cook County State's Attorney's Office, Chicago, Illinois	936, 961
Jaffe, Joseph, Assistant United States Attorney, Southern District of New York	1327
Jamil, Ben, Communications Control Corporation	1400
Joiner, Hon. Charles W., U.S. District Court Judge, Eastern District of Michigan, Detroit, Michigan	524
Joyce, Edward T., Deputy Chief, Organized Crime and Racketeering Section, U.S. Department of Justice, Washington, D.C.	889
Kaiser, Martin L., President, Martin L. Kaiser, Inc.	1400
Kelley, Clarence M., Director, Federal Bureau of Investigation	93
Kelly, John, Supervisor in Charge of Special Investigations, Organized Crime Division, Federal Bureau of Investigation	93
Kotoske, Thomas E., Attorney-in-Charge, San Francisco Organized Crime Strike Force, U.S. Department of Justice	913
Lapidus, Edith, Professor, Queens College, New York	1063
Lazarus, Jack, District Attorney, Monroe County, New York (Rochester).....	315
Leff, Laurence, Executive Assistant, Nassau County District Attorney's Office, Nassau County, New York.....	829
Leval, Pierre, First Assistant District Attorney, New York County, New York.....	321
Linehan, John P., Professor, Seminole Junior College	1596
Lordi, Joseph, County Prosecutor, Essex County, New Jersey (Newark).....	309
Lynch, William S., Chief, Organized Crime and Racketeering Section, U.S. Department of Justice...	5
Lynn, Carroll M., Chief of Police, Houston, Texas	1277
Macdonald, David R., Assistant Secretary of Enforcement, Operations and Tariff Affairs, U.S. Department of the Treasury	128
Markle, Arnold, District Attorney, New Haven County, Connecticut.....	361

	Page
Martin, Ronald G., Investigator, New York State Police....	654
Matthews, John, III, Director, City-County Strike Force, Essex County Prosecutor's Office, Newark, New Jersey	335
McCarthy, William P., Former Deputy Police Commissioner of New York City	642
McFadden, Daniel, Lieutenant, Organized Crime Unit, Philadelphia Police Department, Philadelphia, Pennsylvania.....	954
Merola, Mario, District Attorney, Philadelphia, Pennsylvania.....	297
Miles, Evan, Captain and Chief Investigator, City-County Strike Force, Essex County Prosecutor's Office, Newark, New Jersey.....	685
Mitrano, Vincent, First Assistant District Attorney, Monroe County, New York.....	335
Modesitt, Billy E., Special Agent, Drug Enforcement Administration, Detroit, Michigan; former U.S. Customs Agent.....	172
Mollen, Hon. Milton, Justice of the Supreme Court of the State of New York, Kings County	550
Morrissey, Michael J., formerly of B.R. Fox Company, Inc	1247
Naruk, Hon. Henry L., Judge, Superior Court of Connecticut, Middletown, Connecticut	576
Nesbitt, H. Philip, Assistant Director of Investigations, Pinkerton's, Inc.....	1452
Nicholson, Robert, Detective Sergeant, New York City Police Department, New York County District Attorney's Squad, New York, New York.....	413
O'Brien, Neil, Executive Assistant District Attorney, Queens County, New York	385
O'Malley, James K., Esquire, Defense Attorney, Pittsburgh, Pennsylvania.....	618
Petersen, Henry E., Assistant Attorney General, Criminal Division, U.S. Department of Justice.....	5
Phillips, Joseph, Chief Assistant to the Special Prosecutor for Corruption, New York	366, 390
Phillips, Walter M., Jr., Special Prosecutor for Corruption, Philadelphia, Pennsylvania	973
Reynolds, James, Attorney, Criminal Division, U.S. Department of Justice	1478
Richards, Peter, Associate Director, Organized Crime and Special Prosecutions Section, Attorney General's Office, New Jersey	353, 390
Saxbe, William B., United States Attorney General	19
Schlam, Peter, Assistant United States Attorney, Brooklyn, New York	909
Schneider, Jerry N., President, Jerry Schneider & Company	1365
Schwartz, Herman, Professor, State University of New York at Buffalo, School of Law.....	1088
Seeley, Albert W., Chief, Special Investigations Branch, United States Customs Service, Washington, D.C.....	818
Simon, Michael, Special Agent, Federal Bureau of Investigation, Las Vegas, Nevada.....	1647
Specter, Arlen, former District Attorney, Philadelphia, Pennsylvania.....	259
Speriglio, Milo A., Director and Chief, Nich Harris Detectives, Inc.....	1452
Stern, Hon. Herbert, U.S. District Court Judge, District of New Jersey	995
Sullivan, Hon. Joseph, Justice of the Supreme Court of the State of New York, Bronx County	568
Sweeney, Robert G., Supervisor, Organized Crime Division, Federal Bureau of Investigation, New York, New York.....	855
Tammamo, Richard, Special Agent, Federal Bureau of Investigation, New York City Division.....	413

	Page
Thompson, James, R., Jr., United States Attorney, Northern District of Illinois.....	965
Uviller, Richard, Professor, Columbia University School of Law	1048
VanDewerker, John S., General Manager, System Division, Ashby & Associates.....	1263, 1400
Vernier, Theodore L., Regional Director, Drug Enforcement Administration, Detroit, Michigan.....	718
Wampler, Atlee, III, Attorney-in-Charge, Miami Organized Crime Strike Force, U.S. Department of Justice	172
Worden, Gary G., Section Chief, Technical Operations Division, Drug Enforcement Administration, Washington, D.C.	747

Statements by Nonwitnesses

Frank Rogers, New York Special Narcotics Prosecutor	382
Telford Taylor, Professor, Columbia University School of Law	984
J. R. Ormesher, Assistant District Attorney, Dallas County, Texas.....	985
Stephen J. McEwen, Jr., District Attorney, Delaware County, Pennsylvania	986
William J. Guste, Jr., Attorney General, State of Louisiana.....	987
Harry F. Connick, District Attorney, New Orleans, Louisiana.....	988
Richard B. Allyn, Assistant Attorney General, Office of the Attorney General, State of Minnesota.....	990
Theodore I. Koskoff, Chairman, Chief Justice Earl Warren Conference on Advocacy, Roscoe Pound- American Trial Lawyers Foundation	990
James G. Carr, Associate Professor and Director, Criminal Law Practice Program, University of Toledo College of Law.....	990
Rowland F. Kirks, Director, Administrative Office of the United States Courts	994
Herbert J. Stern, United States District Judge, District of New Jersey	995
Edward H. Levi, Attorney General of the United States	1007
Carol Vance, District Attorney, Harris County, Texas	1302

Hearing Days

September 16, 1974	1
September 17, 1974	93
December 2, 1974	127
December 3, 1974.....	128
March 18, 1975	254
March 19, 1975	352
March 20, 1975	413
April 22, 1975	523
April 23, 1975	618
May 19, 1975	717
May 20, 1975	835
May 21, 1975	889
June 9, 1975	919
June 10, 1975	983
June 11, 1975	1063
June 25, 1975	1150
June 26, 1975	1345
June 27, 1975	1478

Hearing, Tuesday, May 20, 1975

Washington, D.C.

The meeting was reconvened at 9:30 a.m., in Room 318, Russell Building, William H. Erickson, Chairman, presiding. Commission members present: William H. Erickson, Chairman; Chief Richard R. Andersen, Professor G. Robert Blakey, Samuel R. Pierce, Jr., Professor Frank J. Remington, Ms. Florence P. Shientag, Alan F. Westin.

Staff present; Kenneth J. Hodson, Esq., Executive Director; David Cook, Esq.

PROCEEDINGS

CHAIRMAN ERICKSON: The Commission will come to order.

We are honored today to have a number of representatives from the Federal Bureau of Investigation who will offer the Commission information and advice regarding Title III in areas that have come about from staff investigation that would go to the effectiveness of this legislation as a means of effectively dealing with organized crime and as a means of pursuing effective law enforcement while not violating the reasonable needs for privacy.

The first witness that we have this morning is William Cleveland, Assistant Director of the Federal Bureau of Investigation.

Mr. Cleveland, we are pleased to have you here. Would you be sworn, sir?

[Whereupon, William Cleveland was duly sworn by the Chairman.]

TESTIMONY OF ASSISTANT DIRECTOR WILLIAM V. CLEVELAND, FEDERAL BUREAU OF INVESTIGATION, ACCOMPANIED BY ALVIN A. STAFFELD, INSPECTOR, AND JOHN E. KELLY, JR., INSPECTOR, FEDERAL BUREAU OF INVESTIGATION

CHAIRMAN ERICKSON: As I understand it, you have a prepared statement that you are going to offer.

Is that ready for distribution or do you have copies for Commission members?

MR. CLEVELAND: Yes, it is.

CHAIRMAN ERICKSON: We are indebted to you for preparing a statement in such detail, and it will be very valuable to us, and at this time, with

the Commission's permission, if I hear no objection, I will suggest that this be included as part of the record and as part of the proceedings of this Commission.

Hearing no objection, it will be filed and included as a part of the record of this Commission.

Mr. Cleveland, I don't know how you desire to proceed, but to try to save time—I know how committed you are—if it is agreeable to you, I would appreciate your hitting the highlights of this by way of some preliminary remarks, and then upon completion of those remarks, Mr. Cook of our staff will ask some preliminary questions, and then the Commission itself will proceed to interrogate you on your prepared statement and on the areas that we have reviewed with you previously.

MR. CLEVELAND: All right, sir.

Mr. Chairman, I was asked specific questions in connection with this appearance, and this statement includes the answers to some of those specific questions. It is fairly brief, so if I may, I will read it.

When Congress enacted the *Omnibus Crime Control and Safe Streets Act of 1968* it was obvious that some concern existed on Capitol Hill about the possible abuse of electronic surveillances. And well it might have, considering the advanced state of technical developments in recent years and the large number of law enforcement agencies employing these sophisticated listening devices.

Counterbalancing this concern, however, was the undeniable fact that society needed protection from such pervasive evils as organized crime, and that electronic surveillances provide the Government with one of the most effective weapons in its legal armory.

Organized crime, by its very nature, is a vast conspiracy which does not lend itself to investigative techniques aimed at lone-wolf car thieves, bandits, burglars, and muggers. It is big business in every sense of the word, and its members often enjoy positions of power, as well as great respectability, in their local communities. Furthermore, its leaders exercise such a strong control over their operations that potential witnesses are justifiably reluctant to testify for fear of jeopardizing their lives or those of their families. And physical surveillances are extremely limited in effectiveness, since they can determine who is meeting with whom but rarely what is said.

As a result of all these obstacles, our experience in the FBI has shown that electronic surveillances are one of the few investigative techniques to consistently hit the underworld where it hurts and, because of this, there are few things more uniformly feared by the hoodlum element. No bookmaker of any consequence can operate without his telephone network, and, by and large, Title III of the Omnibus Crime Control and Safe Streets Act effectively cuts into these networks.

Conscious of two such conflicting concerns—one for the preservation of individual privacy and one for the protection of society against mobs of ruthless killers—the FBI has instituted various procedures to safeguard the former without endangering the latter in the use of Title III.

Needless to say, initial action in these investigations commences on the field level, and a number of our representatives from around the country have been invited here to testify before you and answer any questions you may wish to ask them. Certainly it is they who know their subjects best and who have determined which investigative techniques will be most productive in their local situations, and who have worked with the United States Attorney or Strike Force Attorney on the scene to draw up requests for Title III authorization. It is also they who go to the judges for court orders after the Attorney General has granted approval, and it is they who supervise the actual operation of the electronic surveillances and the investigations stemming from them.

My purpose in appearing here before you today is to discuss the supervision and review of these activities from a headquarters level.

Basically, Headquarters' control of electronic surveillances is threefold: case supervision, legal review, and executive approval or disapproval.

When a Title III affidavit is received at FBI Headquarters, it is closely scrutinized from the casework standpoint in the unit and section levels to insure that the factual material is accurate, that the probable cause is current and adequate, that the case is of sufficient importance to warrant such coverage, and that an electronic surveillance is necessary to bring the investigation to a successful conclusion.

Because our experience on a national level gives us a broad overview not available in any one field office, we are particularly well situated to compare hoodlum operations in various parts of the country and evaluate their relationship to the organized crime structure as a whole.

Through this nationwide experience we are also better able to analyze the preparation of each affidavit for content than is the supervisory staff in a

given field office, which handles only a fraction of the number of affidavits in a year that we do.

In addition, being removed from the actual investigation of the case itself, we can often form a more objective appraisal regarding the statutory provision that, before electronic surveillance be resorted to, the applying agency must certify that normal investigative procedures are either too dangerous or are unlikely to succeed.

With respect to probable cause, our headquarters staff reviews all Title III affidavits for adequacy as well as to make certain that they meet the Department's 21-day rule. Under this guideline, the Department has stipulated that no more than three weeks may transpire between the date of the last information relating to probable cause in the affidavit and the time the affidavit itself reaches the Attorney General's desk for approval.

Because of our broad overview experience in these matters, we have also encountered several instances wherein the field apparently failed to realize that the probable cause in its affidavit was so overwhelming that it did not need a Title III at all. It already had enough information to either apply for a search warrant or to go before a Federal Grand Jury for a possible indictment. In such cases, we decline the field's application and suggest what we believe is a more appropriate course of action.

On the second level of Headquarters' control of Title III applications is the review of the affidavit by our Legal Counsel Division, which has the overall responsibility of insuring that these documents are legally sound in all aspects and ready for presentation to the Attorney General.

The third and last level, of course, is the executive approval or disapproval of the affidavits, based on a thorough review by myself, as Assistant Director, by the Deputy Associate Director-Investigative, by the Associate Director, and finally by the Director, himself. This is in keeping with the Departmental guidelines that Title III requests come from the "highest ranking officer of the agency with jurisdiction over the offense in connection with which the interception is to be made."

The qualifications of the reviewing officials on the various levels at Bureau Headquarters include a broad spectrum of experience, ranging from previous field practice at installing and operating Title III surveillances to a high-level oversight background in examining and approving more than 800 such applications during the past six years.

We have also, through this long experience, learned many valuable lessons and, I think, improved our operations as a result.

Probably the most important discovery we made in this respect was that electronic surveillances are

expensive and require great expenditures of manpower. When a small office applies for one, we have to transfer in a number of agents from surrounding offices on a temporary basis or else the rest of the work of that office would suffer substantially. Altogether, Title III operations have cost the FBI approximately \$6.4 million in manpower and resources since 1969.

On the other hand, fines and confiscations of cash, property, weapons, and wagering paraphernalia stemming from Title III investigations during the same period have amounted to more than \$8.4 million or a "profit," you might say, of some \$2 million. But even if we received no return at all on the money spent, it should be borne in mind that electronic surveillances may be utilized only as a last resort and that the 1,300 subjects convicted as a result of Title III evidence in FBI cases would undoubtedly never have been convicted otherwise. Furthermore, we should also remember that these 1,300 subjects include some of the top names in the American underworld. How do you place a dollar-and-cents value on that?

From the standpoint of experience, we have been improving with each passing year, so that affidavits are now better prepared in the field and fewer have to be turned down on the headquarters level because of errors, faulty probable cause, missing elements, or the like.

In the operation of the electronic surveillances themselves, our field agents have gradually learned how to minimize the number of interceptions, so that extraneous messages may be cut off as quickly as possible, coverage of pay booths is restricted to specific times, and monitoring is discontinued as soon as a violation has been established and all the members of the conspiracy have been identified.

Naturally, as our intelligence in the field of organized crime increases, we have been able to target our investigations more effectively, so that we are now in a better position to stress quality rather than quantity. And that is essential if you really hope to make any serious inroads in the activities of major criminal groups operating throughout the country at this time.

Just recently, in fact, penetrative Title III coverage by the FBI led to the indictment of 24 persons charged with conducting the largest book-making and policy operation in the Metropolitan New York City area. It has been estimated that the ring—which had close Syndicate ties—was handling at least \$100 million a year in wagers.

Investigations of this sort have not only enabled the Bureau to increase its effectiveness in the fight against organized crime but have also confirmed our previous findings that gambling is the federal

offense most susceptible to Title III coverage and the one most devastated by it.

Obviously, as provided for in the Omnibus Crime Control and Safe Streets Act, we have employed electronic surveillances against hoodlum loan sharks, extortionists, criminals dealing in interstate transportation of stolen property, and the like but, as a rule, we found that few criminals rely as exclusively on telephonic communications as do large-scale bookmakers.

Since these gamblers provide the underworld with a substantial amount of its illicit revenue, they constitute one of our foremost targets. And our efforts to combat them would be seriously impaired without the use of Title III. Therefore, we would hate very much to lose such a valuable investigative tool, and we have taken every possible precaution to insure that it is used in strict conformity with the law.

Now, in reply to certain questions raised by the Commission prior to my appearance here today, I would like to state that I am an Assistant Director of the Special Investigative Division. Under my direct supervision are the activities of three sections, one of which deals exclusively with organized crime violations. In this section are a Section Chief, his Number One Man, and four units—consisting of a total of four Unit Chiefs and nine Supervisors—all of whom are charged with the review of Title III applications, depending upon the geographical location of the submitting field office. Of these 15 supervisory officials, more than half have had direct experience as Title III case agents or affiants in the field, and all have had broad supervisory experience either in the field or here at Bureau Headquarters. Their length of service ranges from 10 years' agent time to more than 30.

As regards the reviewing personnel in the Department's Organized Crime and Racketeering Section, we work quite closely with them on each request, and our standards and considerations are substantially the same as theirs.

Although we keep no precise figures on the percentage of affidavits which are modified at headquarters level for reasons other than style and typographical errors, I think a fair estimate would be approximately 20 to 30 per cent for the larger, more experienced offices and 60 to 70 per cent for the smaller offices which have handled fewer Title III installations. Most of the requested changes deal with such things as updating the probable cause, establishing the informant's position and the basis of his knowledge, meeting the requirements of the statute, and naming all the principals in a gambling operation, rather than the minimum specified in the Organized Crime Control Act of 1970.

In addition, after leaving the Bureau, these affidavits go to the Criminal Division of the Department of Justice where other changes may be suggested.

With respect to the possibility of shortening the review process, our Director, Clarence Kelley, testified before this Commission last September that he thought the present procedures were absolutely necessary. I agreed fully with Mr. Kelley at the time, and there has been no change in the Bureau's position since then.

Congress and the public are both concerned about the impact of electronic surveillances on the issue of individual privacy, and I do not believe that we should do anything to relax the safeguards now employed to oversee these operations.

The law is a good one. It is functioning effectively. It has survived every legal challenge to date. It has met the test of time. I see no reason to make any serious alterations in it.

Now, Mr. Chairman, I would like to introduce my Deputy, Number One Man Inspector Al Staffeld on my left, and Inspector John Kelly on my right. And we have four supervisory agents from field offices throughout the country seated behind us. We have James Esposito, from Detroit; Benjamin Grogan from Miami; Robert G. Sweeney from New York; and John R. Barron from Los Angeles.

I hope among these we can answer your questions.

CHAIRMAN ERICKSON: Thank you. Do you feel that each of these will be volunteering information at some stage or that they may?

MR. CLEVELAND: I think that they will.

CHAIRMAN ERICKSON: Then may I ask that they all be sworn at this time?

[Whereupon, Alvin A. Staffeld, John E. Kelly, Jr., Robert Sweeney, John Barron, Benjamin Grogan, and James Esposito were duly sworn by the Chairman.]

CHAIRMAN ERICKSON: Now, to proceed with staff questions before pursuing questions on an individual basis from the Commission members.

And I might say I am still rather embarrassed by the attendance of the Commission members. We have eight Congressional members that I hoped would be in attendance since this is extremely important testimony. We do have a number of our public members present, but I hope the remaining members will be here before the testimony is completed.

Mr. Cook.

MR. COOK: Thank you, Mr. Chairman.

Mr. Cleveland, referring to your statement and the impact of the *Omnibus Crime Control and Safe Streets Act of 1968* upon the state of electronic sur-

veillance at that time, can you give the Commission some idea of what the Bureau's practices were in the field of electronic surveillance prior to the enactment of the Act, and how do you interpret the existing law as to apply to your own practices?

MR. CLEVELAND: Just prior to the enactment of the Act our electronic surveillance coverage in criminal matters was practically non-existent.

MR. COOK: Was this due to Justice Department policy at that time?

MR. CLEVELAND: Yes, mainly.

MR. COOK: It was not immediately upon enacting the statute that you did become active in electronic surveillance; is that correct?

MR. CLEVELAND: Upon enactment of this particular legislation there was still a period when there was no electronic surveillance coverage. In 1969, the first installation was made under the Act.

MR. COOK: Do you recall and have any figures at your disposal which would indicate the number or frequency of installations which you used in the early stages of the Act in 1969?

MR. CLEVELAND: I don't have the figures at my disposal. There have been over 800 since 1969. There was a period of activity in 1971 where we had more than we have had before or since, but other than that they have been pretty well stable.

MR. COOK: When you first began to implement the statute and your own agency began electronic surveillance operations, what was the nature of your approach to this job? Was this something which you were technically unprepared for at that time, or did you have a pretty good idea of what needed to be done under the statute?

I am trying to get at the learning process which you indicated, that you had learned some things about electronic surveillance.

MR. CLEVELAND: Technically, we were quite well prepared. From the standpoint of the statute, itself, and the preparation of affidavits, the obtaining of probable cause, this obviously was new and the gambling cases were new insofar as the FBI was concerned, and there was a learning process involved there.

MR. COOK: Now, you had been an agent in the Bureau prior to the use of any electronic surveillance, isn't that right, an enforcement officer?

MR. CLEVELAND: I beg your pardon?

MR. COOK: Were you not an enforcement officer in the FBI before the enactment of the Electronic Surveillance Act?

MR. CLEVELAND: Yes.

MR. COOK: And did you have experience in the organized crime field prior to the enactment of the 1968 bill?

MR. CLEVELAND: The gentlemen here, particularly Mr. Staffeld and Mr. Kelly, on my left and right, were far more active in it prior to 1968 than I was.

MR. COOK: Could you give, perhaps among the three of you, some idea of the procedures which the Bureau relied on in organized crime investigations before it had available to it electronic surveillance?

MR. STAFFELD: Our interest in organized crime, of course, went back to 1957, after that famous Apalachin meeting. And we found at that time it was very difficult to get any basic intelligence information with respect to organized crime, itself. Physical surveillances and record checks didn't produce the material, the meat that we wanted. And as a consequence, we were authorized—oh, I believe it was in the late '50's or early 1960's—to use electronic surveillance techniques for the purpose of gathering intelligence.

After a period of time, and in fact up to July 12, 1965 we did use that technique, but on July 12, 1965 it was discontinued and we had not used that technique until the Title III provisions were enacted.

MR. COOK: Your use of the technique at that time was under the authority of the Justice Department?

MR. STAFFELD: That is right, sir.

MR. COOK: And the context in which that was carried out at the time was that interception was permitted but that divulgence was not; is that right?

MR. STAFFELD: That is correct.

MR. COOK: Now, in addition to your activities in electronic surveillance, what conventional means did you rely upon in enforcement of organized crime laws before enactment of the 1968 bill?

MR. STAFFELD: Well, this would include the good old hard-nosed investigations, the physical surveillance, the observations and, of course, the inclusion of informant information that you can develop from time to time. And then the privilege of search warrants would also help out in the obtaining of the necessary evidence.

MR. COOK: Is there any basis upon which you could compare your effectiveness at that time in organized crime investigations to the effectiveness which the Bureau seemed to enjoy in areas such as bank robbery, interstate theft, stolen cars, and so forth?

MR. STAFFELD: In the absence of the Title III privilege?

MR. COOK: That is right.

MR. STAFFELD: Well, I am quite certain that what we were after were the kingpins in organized

crime. And we were unable to penetrate that area of insulation which existed between the street gambler and the kingpin or the boss.

So I don't think that prior to the enactment of Title III we were as successful in getting the big people. Later, with the Title III, we were able to penetrate deeper into the organization.

MR. COOK: And when was it that the Bureau obtained jurisdiction in interstate gambling?

MR. STAFFELD: In the fall of 1961.

MR. COOK: It was in 1970 that the Bureau obtained jurisdiction in the illegal gambling business?

MR. STAFFELD: Right.

MR. COOK: So that your investigative techniques against organized crime or your jurisdiction, I should say, was enlarged by statute prior to enactment of the Organized Crime Act of 1968?

MR. STAFFELD: Yes, it was.

MR. COOK: Okay. With reference to the advanced state of technical development which Mr. Cleveland referred to, how does the Bureau structure its apparatus for insuring that its own technology is adequate to keep up with the investigative needs in the field?

MR. CLEVELAND: Are you speaking of the actual mechanical techniques now?

MR. COOK: Well, for example, does the Bureau have—I know they have a national crime laboratory, a forensic-type service which it offers to local and state police departments.

MR. CLEVELAND: Right.

MR. COOK: Do you have similar technical apparatus which you rely on to assure you have a technological capability in electronic surveillance?

MR. CLEVELAND: Well, I think you would have to say that the procedure of keeping up is a constant training procedure, which we do have, ranging from our new agents right through to our experienced agents operating in organized crime.

The laboratory likewise keeps tabs with all new developments and is right up to scratch on those things.

Does that answer your question at all?

MR. COOK: Yes, I think it gets into the area.

What type of personnel are employed in your laboratory who are devoted to the development of your technological capability in electronic surveillance? Are these engineers?

MR. CLEVELAND: Engineers, scientists, yes. And I think a group of representatives from our laboratory appeared before this Commission and gave testimony in depth as to their operations in connection with Title III. And they, of course, are a little bit better qualified to speak on their operations than are we, their operations being engineering and technical to a large degree, whereas ours is more or less investigative.

MR. COOK: Do you have procedures whereby you insure that the latest in technological developments can be deployed by your investigative personnel, in other words, that they don't just blossom in the laboratory and never hit the streets, so to speak?

MR. CLEVELAND: Yes, we have laboratory technicians instructing our agents who are operating in organized crime matters regularly. And they actually go to the field on many occasions and work on installations that are necessary in connection with specific operations.

MR. COOK: So do you have a—perhaps job classification is the wrong word—but do you have personnel who function as training people in the technical area to insure you have a field operation capability which is up to date with your technological achievements?

MR. CLEVELAND: Absolutely right.

MR. COOK: And in terms of the dynamics of an ongoing investigation I take it you may have demands in different cities for various types of equipment—cameras or video-tape or bugs, and so forth?

MR. CLEVELAND: Where that happens, the field only has to let us know and the laboratory will see to it that that equipment is sent promptly to that particular area, along with a technician, if necessary, to help in the installation.

MR. COOK: Is the bulk of your sophisticated equipment maintained centrally in Washington?

MR. CLEVELAND: No, it is located throughout the field—and based on prior needs, there is a certain amount of equipment in each of our 59 field offices.

You develop a history of need in various areas. And Detroit may have far more electronic equipment or technical equipment than does Savannah, for example. And based on those needs, the equipment is there.

When they need more, Washington will send it out.

MR. COOK: Do you ever have occasion to exchange or compare with other Federal investigative agencies, such as the Drug Enforcement Administration, their own developing capabilities in this area?

MR. CLEVELAND: We do that regularly. Our laboratory technicians are in touch with their laboratory technicians and Mr. John Kelly, here, maintains close liaison on the headquarters level with the DEA from an investigative standpoint. We are in close touch with each other.

MR. COOK: Have you found this to be of mutual benefit?

MR. CLEVELAND: Mutual benefit. Indeed, it is.

MR. COOK: One of the remarks in your statement went to the effect that a determination was made in the reviewing process as to whether the application was a suitable one for deployment of Title III. And I take it—and correct me, if I am wrong—that this is a policy determination more than a probable cause determination; is that right?

MR. CLEVELAND: Well, starting with the statute, itself, we want to be sure that it is the type of case that is covered by the statute. That is number one.

And we go from there.

It may be that from experience by personnel here at Headquarters a different approach might be appropriate for a particular case—or it may be from reviewing material that they have already obtained through investigation that there is no need for Title III.

We have to satisfy ourselves that according to the statute there is no other logical way of obtaining the information other than Title III.

MR. COOK: Well, is your manpower adequate—have you made a policy judgment that, for example, all gambling operations which fall within the ambit of the statute of 1955 are an appropriate subject for electronic surveillance?

MR. CLEVELAND: No, not at all. All gambling subjects would not be proper subjects for Title III installations. We try to restrict our gambling cases to quality type solely, no "Mom and Pop" operations, no little old lady at the candy store. It has to be targeted toward persons who are operating on a rather high level in a syndicate or someone who is operational in a very large gambling ring to warrant the use of Title III, we feel.

MR. COOK: So your reviewing section has to have some kind of fairly close liaison with an intelligence function; is that correct?

MR. CLEVELAND: Yes, indeed.

MR. COOK: As to the importance of the applications you receive?

MR. CLEVELAND: Absolutely.

MR. COOK: Do you rely more on the input of the field appraisal, in other words, the people who gather the intelligence in the field, or do you rely on centralized files which would represent what you have already accumulated in terms of intelligence about gambling operations in a particular area?

MR. CLEVELAND: We have a centralized system in the FBI unlike some other government agencies who are compartmentalized or operate on a regional basis. We operate solely on a centralized concept in the FBI. So the information being reviewed at headquarters is information gleaned from all our 59 field offices and maintained on a central level from that review a determination is made.

MR. COOK: In other words, if an application came into your office from, say Chicago and it named as its principal subject John Doe, would you have the capability at Headquarters of making a complete intelligence check on John Doe and his significance in organized crime in Chicago at Headquarters?

MR. CLEVELAND: Normally that would be possible, yes, not only from information from Chicago, but information that might come in from Los Angeles or New York or other offices relating to John Doe. It would all be considered in our centralized check of records.

MR. COOK: You would then have access to information from other cities which the field office originating the application would not have?

MR. CLEVELAND: That is many times correct—not always correct, however, because if two field offices know of the same subject more than likely those two field offices would have the same information about that subject. But that is not always true. So the only way to have a complete check of everything the FBI knows about an individual is through a check of the central files here.

MR. COOK: In assessing the importance of electronic surveillance, is there a flow through field offices independent of intelligence input to Headquarters? In other words, would Detroit and Chicago have an intelligence liaison independent of the files that have been sent to your Headquarters?

MR. CLEVELAND: Not normally. Normally any intelligence information developed by Detroit and Chicago about a particular individual would also be channeled into Headquarters.

MR. COOK: In terms of data retention and retrieval, what kind of capability do you have? Do you have a computerized capability as far as intelligence assessments are concerned?

MR. CLEVELAND: No, sir, we do not.

MR. COOK: You have to run a manual file check?

MR. CLEVELAND: Right.

MR. COOK: Do you ever find that this slows down the process?

MR. CLEVELAND: I don't think so to that degree. I think it is very necessary to be able to manually retrieve intelligence information on an organized crime subject for a thorough view. Sure, certain key things can be computerized and are computerized. In the Justice Department, for example, they have the computerized racketeer profile. But to have a complete review of all information available about an individual, I personally would like to see the whole file and not just some key things that were punched into a card and computerized.

MR. COOK: Do you rely to any extent on the Racketeer Profile System the Justice Department uses?

MR. CLEVELAND: No, sir. A large percentage of the information going into their computers is taken directly from FBI reports.

MR. COOK: You mentioned the 21 days which the Justice Department has mandated for probable cause. In our interviews in the field in some of the major cities there were indications that particularly in theft and fencing operations, the frequency of the commission of the offense was not of a daily nature which characterizes a gambling business. In other words, there might be a theft the first day of the month; it might not come again until the 30th day of that month. And the sale of those goods and passing on of those goods to a fence or buyer might take place even as long as three or four weeks later.

Do you think, or have you found a need, based upon the intelligence which you have received, and the theft and fencing applications which you have received, to relax the 21-day requirement in cases such as these where there is not a daily ongoing business?

MR. STAFFELD: I think the rule is an administrative rule that is established by the Department of Justice right now, and I think it has been utilized because it has been workable in our type of case. We haven't had a great deal of experience with the Title III in connection with theft from interstate shipment or bank robbery or anything else. It is a different kind of a crime. It is not a constant, ongoing thing.

I would expect that if there was some solid information respecting pertinent conversations that were outside of the 21 days—I would think that there would be some leeway. I think that it would be part of the probable cause. So I don't know that it would be necessary to relax or revise that particular administrative rule. I couldn't say.

MR. COOK: But you think there might be occasions where there would be suitable exceptions to the rule?

MR. CLEVELAND: Oh, I think there could be, yes.

MR. COOK: Mr. Cleveland, you made reference to the amount of money expended on electronic surveillance by the Bureau and—let me get the correct figure here—\$6.4 million in manpower and resources since 1969. Can you give the Commission any idea how this compares with the allocation of manpower and resources to the conventional means of investigation during the same period?

I realize you may not have budget figures in front of you—

MR. CLEVELAND: No.

MR. COOK: Is this something you could provide the Commission with—a comparison of the expenditures made by the Bureau on electronic surveillance with the expenditures made by the Bureau in other conventional areas?

MR. CLEVELAND: I don't know—number one, yes, we can furnish figures relating to expenditures in connection with various types of investigative operations of the FBI. True, we can do that.

I don't know of any figure, however, that has compared cost of Title III operations with any other specific type operation, any one of the 180 Federal violations that we handle.

But there are cost figures relating to the various operations. There is a cost figure for organized crimes; there is a cost figure for white collar crimes; there is a cost figure for general crimes of a specific name—things of this sort. If this would be of any help to you, there are those figures available from our budget.

MR. COOK: I think this would be of help to the Commission, and I think you recognize the point of the question is in comparing the strain on the budget of the Bureau for expenditure on Title III in comparison with expenditures on conventional means might give us some kind of figure on the return that is obtained in terms of convictions or indictments or disruptions of organization—whatever criteria one might use to measure the success. We would then have to bring that back to the cost of the efforts.

MR. CLEVELAND: You would have to say an expenditure of \$6.5 million since 1969 would be a figure of way less than 1 per cent of the cost of other operations in the FBI.

MR. COOK: Less than 1 per cent?

MR. CLEVELAND: Oh, it would be less than 1 per cent, I'm sure.

MR. STAFFELD: I am wondering, Mr. Cook. Are you asking to compare the cost of a gambling investigation with the cost of a bank robbery investigation? Or are you asking to compare a gambling investigation wherein there is no Title III use with one where there is?

MR. COOK: I would say both comparisons would be meaningful.

MR. STAFFELD: I think if you are going to compare a gambling case with a bank robbery case, you have apples and oranges, really.

MR. COOK: Then I think perhaps it should be restricted to a context of use of electronic surveillance versus use of conventional means.

PROFESSOR BLAKEY: Mr. Cook, would you mind if I asked a question?

MR. COOK: Certainly, Professor, go ahead.

PROFESSOR BLAKEY: When people see a figure of \$6 million, they tend to compare it with their personal income and when I think of \$6 million, that is a lot of money, and the attitude is, "That's awfully expensive." Most people who genuinely want to understand criminal investigations and this kind of criminal investigation in particular, need a context, that is, they need a feel for how expensive a bank robbery investigation is, the typical one. It could give them a feel for how expensive investigations are, that is, a feel for how expensive a gambling case with a wiretap is as against a gambling case without a wiretap.

The figure you just gave us, for example, that this is less than 1 per cent of the Bureau's operation, suddenly throws us into sharp relief that while \$6 million is very expensive if you match it against my personal income, as against the operational costs of the FBI, it is not fairly large or fairly expensive.

And I think perspective is what the Commission needs to have in discussing investigations and the cost of investigations.

But simply citing the figure—I think the figure for the cost of an average Federal wiretap is \$5,000 or \$6,000. That sounds like an awful lot of money. Yet I have seen figures indicating that in the Strike Force in Chicago the average Strike Force investigation costs \$200,000. Now, \$5,000 or \$10,000 thrown against \$200,000 indicates that this is one alternative that, while expensive in terms of personal income, is not expensive in terms of a general cost framework.

That is what Mr. Cook would like to have some rough estimates on, so the record can reflect the proper values.

MR. CLEVELAND: Professor Blakey, what you say points up a problem we have in the budget area. We are sometimes asked to come up with a case-by-case figure of what certain types of investigations cost. This is a most difficult thing to do, and I think you can understand readily why. You can have one case that costs \$1,000 and then the Patty Hearst case comes along and it costs millions. Or you can have a routine background Presidential appointee-type investigation on an individual for which we charge a little over \$2,000, and then along comes the Ford investigation and the Rockefeller investigation that again cost millions of dollars.

So it is very difficult to come up with a case-by-case figure.

So what we have attempted to do, or what the Department has asked us to do is to come up with a cost by man-years on a particular program: How much does the organized crime program cost? How much does the white collar crime program cost on an annual basis?

We can provide this type figure through surveys of manpower use in the field.

But to come up with an individual cost figure by violation is a very difficult thing to do.

PROFESSOR BLAKEY: I think even program cost would put it in context.

MR. CLEVELAND: The program costs we can furnish.

PROFESSOR BLAKEY: To continue this line, for example, to talk about how successful or how expensive would a gambling investigation be without surveillance and noting that throwing the surveillance in may make it twice as expensive is sometimes not helpful. It also may make it successful. And then you are comparing and contrasting a high cost with no success against a higher cost with success. It is only then that it seems to me you have a value context to evaluate the technique.

[The information requested follows.]

WILLIAM V. CLEVELAND

August 8, 1975

General Kenneth Hodson

Executive Director

National Commission For The Review of Federal and State Laws

Relating to Wiretapping and Electronic Surveillance

Room 708

1875 Connecticut Avenue, N.W.

Washington, D.C. 20009

Dear Ken:

In response to your telephonic request of August 5, 1975, the following information was prepared by my staff:

Cost figures incurred in the investigation of an illegal gambling operation utilizing conventional techniques as compared with electronic surveillance methods are not available for analysis due to many changing variables.

An actual case, however, will serve to point out the overall investigative effectiveness of a Title III installation. For two years, prior to 1969, the FBI conducted an investigation to piece together the activities of a major East Coast numbers operation. In June, 1969, armed with the Title III provisions of the Omnibus Crime Control and Safe Streets Act of 1968, the FBI reinstituted its efforts against this combine and within three months from the date of the first court order, more than 55 subjects were indicted by a Federal Grand Jury. To date, 49 of these persons have pleaded guilty, receiving fines totaling \$44,000 and sentences adding up to 100 years in actual prison time and probation.

I trust that the above information will be of assistance to you.

Sincerely,

[signed] Bill

MR. COOK: Thank you, Professor. That elucidates the point I was trying to make.

I just have one further question for Mr. Cleveland. Most of the questions and areas of interest which we submitted to you I think have been answered adequately in your prepared statement.

I did want to ask you if there is any flow of personnel between Division 9, which is the Organized Crime Division, and field supervisors. In other words, would a man who had worked in Headquarters then ever go back out into the field and employ his expertise which he apparently acquired under your supervision in actual field investigations? Is this ever done?

MR. CLEVELAND: Yes, I would almost say, "yes, unfortunately," because, from a strictly selfish standpoint it is invaluable for me to have experienced personnel like Inspector Staffeld and Inspector Kelly at Headquarters and not let them go back to the field.

However, in actual experience and practice we have a development program where inspectors, after coming into Headquarters for a couple of years, are considered for the next step up: The Inspection Staff and, from there, to Special Assistant Agent in Charge in the Field, and then the full Inspector's Staff, and so on.

So there is a constant flow of men coming into Headquarters.

MR. COOK: Do you know how many men crossed this route in the last year, for example?

MR. CLEVELAND: In the last year in the Division 15 to 20 men, I would say, and 5 out of the Organized Crime Section.

MR. COOK: Thank you very much.

CHAIRMAN ERICKSON: Thank you very much, Mr. Cook.

Professor Blakey.

PROFESSOR BLAKEY: Mr. Cleveland, I see from your background that you have been in the Department as a clerk since 1939 and in Special Investigations since roughly 1951.

Now, the Kefauver hearings were held in the early '50s. They were followed by McClellan Committee hearings in the late '50's and early '60's. You were in the FBI and could watch the special group under Attorney General Rogers in its efforts to deal with organized crime. You have had an opportunity to watch the Kennedy program on organized crime in the 1960's. You saw what former Attorney General Clark did or did not do in the organized crime area. You saw the Nixon Administration come in and begin a new drive on organized crime. You have seen the legislative program by Congress begin in the early '60's, go through the Wiretap Act in 1968, and then end with the Organized Crime Control Act in 1970.

What difference has all of this made? I am not talking now about effectiveness or efficiency in the sense that you couldn't get convictions in 1960 and you can get convictions in 1974.

With all of the tools you have had, all of the manpower commitment that you have made, has it really made a difference with organized crime in the street?

MR. CLEVELAND: Yes. One thing I would like to clarify, Professor Blakey, I have been here an inordinately long time, since 1951, but from '51 to '61 I was involved in the Intelligence Division operations, strictly security work. And from '61 to 1970 I ran a section having to do with employee security and special inquiry investigations, Presidential appointees and what not, whereas Mr. Staffeld and Mr. Kelly are far more capable of answering your question since they have been on organized crime for longer as specialists than I.

MR. STAFFELD: I know and recognize that there were times when there was probably not as much enthusiasm in senior levels of the Department as there were at other times. But I think basically once we acquired a foundation of intelligence on what organized crime was and who was involved, I think there was a normal progression toward prosecution.

Now, I do agree that—

PROFESSOR BLAKEY: Mr. Staffeld, I grant there has been a recognition of what is going on. The President's Crime Commission of 1967 laid out the national structure of organized crime and I understand the data in the Report was largely based on the FBI electronic surveillance, and in my judgment, you just can't ignore the nature and scope of the problem you identified and its seriousness. And I am not going to argue with the fact that the Bureau has moved from a handful of convictions in the early 1960's to a substantial number today.

I want to go beyond the question of simple convictions and say: What difference did the convictions make on the organized crime problem in the United States? Are we turning it around?

MR. STAFFELD: Oh, you are talking about the impact of the investigations?

PROFESSOR BLAKEY: Yes. The way it is put to me sometimes is "I grant you wiretapping is effective in the sense it gets evidence, and it leads to convictions, but what difference does it make if you convict a hundred more gamblers? They will just be followed by another hundred gamblers. Consequently, while we are getting gambling convictions, the loss of privacy that we must give up to get them, in light of the fact that we are not turning the gambling problem around, makes no difference."

The same thing can be said in the narcotics area, although I don't expect you to comment on that, and I think the same thing could be said in the fencing area.

So, supposing we use wiretaps in the gambling, fencing, and narcotics areas, are we going to get rid of them? No, and we will just give up a lot of privacy. If we used the conventional techniques, the crime problem wouldn't—

MR. STAFFELD: I think it would. If you are going to use normal techniques and remove the use of Title III, you are going to have a minimum of success against the elite of organized crime.

PROFESSOR BLAKEY: Even if you have maximum success, there are 24 families in La Cosa Nostra. You have had wiretapping authority since 1968. Is a single one of those families out of business?

MR. STAFFELD: Well, there is more than one. It has been quite well decimated. There might be new elements of leadership, not quite as strong, but certainly they are fragmented and in some areas it is at the point where, to accept a position of leadership, is only inviting trouble or a jail sentence.

PROFESSOR BLAKEY: Are you testifying that people are not accepting positions of leadership?

MR. STAFFELD: I think that there are some areas where it is not sought after like it once was.

PROFESSOR BLAKEY: If it is true that some of the LCN families are beginning to be decimated, isn't it also true that Cuban groups, Latin American groups, black groups, are just stepping into their shoes anyway?

MR. STAFFELD: I think in some areas this is true. I think some of the fellows we have from the field could probably give a good answer.

PROFESSOR BLAKEY: Then what difference does it make if we knock out an LCN family in addition to LCN leadership, if it is just succeeded by a Puerto Rican group in New York City. The faces change and the names change and it goes from Italian-American names to Spanish names, but does the problem change?

MR. STAFFELD: The problem doesn't change. You still have an organization you want to defeat and they are operating on a wide level and acquiring a very heavy volume of gambling proceeds. So whether it be LCN or whether it be Puerto Rican or whatever, the problem is still the same. You still want to break it up.

PROFESSOR BLAKEY: Do you offer us any substantial hope of breaking it up by using these sophisticated techniques?

MR. STAFFELD: Well, I certainly do. I don't think we would be in business otherwise if we didn't have some expectation of success.

PROFESSOR BLAKEY: Can you really say to this Commission that wiretapping authority will let you eliminate organized crime?

MR. STAFFELD: Well, Mr. Blakey, I don't think any of us believe that organized crime is going to be totally eliminated.

PROFESSOR BLAKEY: Are you going to be able to substantially reduce it?

MR. STAFFELD: I would hope we can substantially reduce it.

PROFESSOR BLAKEY: Based on your own judgment and experience with your national perspective, do you think we are in fact reducing it now?

MR. STAFFELD: I have been in this business since 1957 and it has a heck of a lot of different complex now than it did back in 1957.

PROFESSOR BLAKEY: Let me put it in another time.

You got in the business, you said, in 1957, at about the time of the Apalachin conspiracy.

I don't want you to put it on a quantified scale, but for the purposes of discussion, put it on a scale of one to ten. How bad was it then? I am also going to ask you in a second to put it on a scale of one to ten today and how bad it is now.

MR. STAFFELD: Well, in '57 I think that—well, all right, let's take '57 and start out with 10 and move down to the present date and I would say that we would have to be better than half-way.

PROFESSOR BLAKEY: To what degree—

MR. STAFFELD: This is just an estimate.

PROFESSOR BLAKEY: I am just asking for an estimate. You are in a position where you have had a chance to see it and look at it. I don't think there is any way we can take an empirical survey.

MR. STAFFELD: I don't think there is, either.

PROFESSOR BLAKEY: Yet it seems to me somewhere along the line we have to ask questions about impact. If all we are going through is a minuet—following the rules, ten levels of review, go out and get the wiretap evidence, get a conviction, and six weeks later, we go through the same process again, then it has no more intrinsic importance than a dance; it is a waste of time, and it is at the cost of a lot of money and a lot of privacy.

But what I am trying to get at is this: To what degree has wiretapping—and by that I mean wiretapping and bugging—contributed to what you are telling me is a kind of turning the problem around?

MR. STAFFELD: I might allude to one of our early cases, I think the Jimmy Nap case, one of our early cases in which we did not have the privilege of Title III. And I don't think we were successful to the extent we wanted to be and this is the case Mr. Cleveland just referred to, \$100 million a year gambling proceeds case, which we were able to get as a result of Title III and we got Mr. Nap in the process.

PROFESSOR BLAKEY: But what was the impact on his operation? So we've got Nap, and Nap went to jail. What about Nap's gambling operation? Is it back in the street now?

MR. STAFFELD: I don't have any idea. I would hope not.

PROFESSOR BLAKEY: Would you think there is a substantial possibility that if he doesn't re-establish it himself or leave it with somebody else while he goes to jail, somebody else will move into the vacuum?

MR. STAFFELD: Let's put it this way. It may well be fragmented. I don't think it will be as large or as sophisticated an organization.

PROFESSOR BLAKEY: What difference does it make if it is large or fragmented, if the same volume of activity is going on?

MR. STAFFELD: I don't say it would be as large. I don't really know.

PROFESSOR BLAKEY: Are you saying then you don't really know—I am troubled with the apparent inconsistency between saying you have cut it from 10 to 5, and now you are saying you don't know what has been the impact.

MR. STAFFELD: You are talking about one particular case.

PROFESSOR BLAKEY: All right. So what you are saying is overall it is your judgment that you have substantially made a difference.

MR. STAFFELD: I would think we have, yes.

PROFESSOR BLAKEY: What would you need to bring it from 5 down to, I take it the irreducible minimum, say 1 or 2? Do you need more manpower? More time?

MR. STAFFELD: Well, I think there is more time and I think that there are a lot of other circumstances that will go with it.

Now, for one thing, early in the game we had some matters of corruption that we had to deal with. I think corruption is something that is more and more being recognized as being brought out in the open and there is being full prosecution of it.

I think when you break that tie of corruption with some officials in the community—

PROFESSOR BLAKEY: It can be police corruption or prosecutor—

MR. STAFFELD: Or political or any corruption. I think if you break that element you are also going to substantially reduce, just normally, the operations of organized criminal gambling combines.

PROFESSOR BLAKEY: Do you see a turning around in that area?

MR. STAFFELD: We have had an awful lot more prosecutions in the corruption category than we used to have, and I think there is a turning point in that.

PROFESSOR BLAKEY: What role does electronic surveillance play in that?

MR. STAFFELD: You pick up the conversations of the person who is doing business or permitting the illegal operation of the combine.

PROFESSOR BLAKEY: I have no further questions for Mr. Staffeld.

Would you like to add anything to that, Mr. Kelly?

MR. KELLY: One thing I might mention, Professor, is when you mention reducing it on a scale of 1 to 10 to 1 or zero, I think basically we have to keep in mind, as you well know, that this is a local problem, too, not just Federal. And all these crimes we are talking about aren't just Federal crimes. They are local crimes.

So as the degree of police efficiency at a local level increases, this has a great impact on the organized criminal element, also.

So it is a combination of local and State authorities and Federal authorities working together.

CHAIRMAN ERICKSON: Let me ask this. Isn't this basically the answer: The fact that law enforcement, regardless of how effective it is, cannot eradicate crime or eradicate organized crime in its entirety, but with effective law enforcement you can control it. You can't eradicate sin, can you? Isn't that the answer?

MR. STAFFELD: I think another part of it is there is a propensity to gamble. There is always a market. And as long as there is a market, as long as somebody wants to bet on numbers or on the stars or something else, there is going to be somebody who is going to be willing to accept that wager.

CHAIRMAN ERICKSON: Right. And the effectiveness of law enforcement provides a means of controlling organized crime and crime. But you aren't going to eradicate it regardless of what you do, isn't that right?

MR. KELLY: Yes, sir.

MR. STAFFELD: That is our view.

PROFESSOR BLAKEY: Let me just ask one last question.

Accepting that as your judgment—and you have been in the Bureau, Mr. Staffeld, for how long?

MR. STAFFELD: A little short of 35 years.

PROFESSOR BLAKEY: To what degree would you say—if you know—would your experience and your judgment be shared by other people in the Bureau? Are you a minority view?

I have asked and gotten now the judgment of a man with 35 years' experience. The next obvious question is: How typical is your experience and your estimation of it?

MR. STAFFELD: Well, Mr. Blakey, first of all, I don't think I have given extensive thought to this

and I would say right off the top of my head we have moved from 10 to 5. Mr. Kelly might say "Well, I think we haven't moved quite that far," or he might feel we have moved farther.

I have not considered with the rest where I stand.

PROFESSOR BLAKEY: I don't want to pin you with the number of 1 to 5 or 10. I just want to talk about order of magnitude. The main question I want to ask is: Have you turned it around and which way are you pushing it? I am not asking you whether the war is over. "War" is probably a bad word to use here. Are you dealing with the problem? Are you beginning to turn it around? Are you beginning to control it? Is it moving from an unfavorable situation to a more favorable situation or are things getting worse? And what can we attribute the improvement to or what can we attribute the decline to?

I am really asking: Has there been a real change in the street as a result of the real change in legislation and law enforcement activity? And you are telling me there has been and it is moving down.

MR. STAFFELD: In my judgment, that is true.

PROFESSOR BLAKEY: All right. Is that general judgment shared by your colleagues?

MR. STAFFELD: I would feel certain it is.

PROFESSOR BLAKEY: Would you disagree with that, Mr. Cleveland?

MR. CLEVELAND: Do I disagree? No, sir.

PROFESSOR BLAKEY: Would you disagree, Mr. Kelly?

MR. KELLY: No, I concur with that.

CHAIRMAN ERICKSON: Mr. Westin.

MR. WESTIN: Mr. Cleveland, I would like to get some idea of how the procedures for FBI use of wiretapping and electronic eavesdropping compared before the enactment of Title III to the procedures afterwards. You described in your statement how things are done now. I wonder if you or your other associates could give us a brief overview of what the procedures were in the late '50's and in the 1960's. I want to contrast then both your supervision and rule structure before and after.

MR. STAFFELD: First of all, we were not in favor of using the electronic surveillance technique at all since there was not a specific law on the books. And we were very confined in our use of the information we acquired from the electronic surveillance technique prior to Title III.

MR. WESTIN: Let me just ask if by electronic surveillance you refer to both the wiretap and the bug?

MR. STAFFELD: Yes.

MR. WESTIN: Thank you.

MR. STAFFELD: I think it was about 1959 or 1960 when we felt a real need for this kind of

coverage. But again, it was extremely closely supervised. Mr. Hoover was not one to tinker with this technique.

It required the field to submit a comprehensive recommendation as to just why they wanted this coverage, where, and how, and for how long, and what did they expect that they would get out of it?

Now, in this particular situation we were looking for intelligence. We couldn't technically disseminate the material, and we couldn't use it for prosecutive purposes.

So we maintained these sources for a period of time until we thought we had exhausted their use and there was no more intelligence to be acquired in that particular spot. Then we would discontinue them, possibly looking for one in another area that would also produce intelligence.

And each case was recommended by the field office to the seat of government. It was reviewed by the various officials on through the Director before the field was notified or authorized to make the installation.

And this, as I say, continued until July 12, 1965, when we terminated all intelligence sources of that type in the criminal field.

MR. WESTIN: That was under the direction of the then Attorney General Ramsey Clark?

MR. STAFFELD: Yes.

MR. KELLY: No, it was Katzenbach.

MR. STAFFELD: Katzenbach, yes.

MR. WESTIN: Would you have any idea whether the length of time of listening tended to be greater or less in certain areas before the enactment of Title III? That is, if you were comparing the electronic surveillance in certain kinds of cases, organized crime or cases that might involve bank robbery and so on, do you have any idea of the length of time of listening before Title III and after Title III?

MR. STAFFELD: I think that we have to grant that under Title III we are looking for specific information, a specific violation. And when that is acquired, we terminate.

Under the other system, the old system, we were looking for intelligence and we weren't required to turn it off at any particular date.

But we always had to bear in mind that these are an expensive use of personnel. So if the device wasn't producing the intelligence that we needed, we would terminate it. But I guess it was longer. I will admit that. It was longer under the old system than under the Title III.

MR. WESTIN: So if one is thinking about duration of time that listening is taking place the contrast between pre-Title III and post-Title III is that the FBI was listening longer in a typical investigation than is the case after Title III; is that so?

MR. STAFFELD: I think that is true.

MR. WESTIN: One of the persistent things that appears in the literature about wiretapping and the FBI, including books by former FBI agents and material that appears in the press, is that because of the absence of a Federal statute, clear-cut, indicating what could be done and what could not be done, and the use of the evidence in court, there was a practice of putting in what we call suicide taps, where agents would, on their own authorization, put an intelligence tap or bug in, knowing that if it was discovered that this would be a cause for discipline or action by the Bureau, but that because of the uncertainty of the law, a feeling that Congress could not make up its mind, and perhaps a feeling that the American public wanted some tapping of this kind done in the interest of law enforcement, there are persistent reports that that was present—unspecified as to how many or at what level.

Did you know of such activity taking place or was it commonly known in the Bureau that this was done occasionally before passage of the statute and Title III?

MR. STAFFELD: First of all, the connotation attached to suicide was if Mr. Hoover found you put one in, it was suicide.

Now, in our program, in our Organized Crime program, we did not resort to the so-called suicide. This was something that was on the record and it was approved by Headquarters.

Now, you say am I aware of any? In the organized crime area, no, but having been in the organization for 35 years, yes, I am aware of some that took place some years ago.

MR. WESTIN: Now, one of the things that was debated when Title III was passed was that Congress specified clearly what crimes you could use interceptions for and what crimes you could not, and if this became the law of the land expressing the will of the Congress and the public behind it, this would stiffen the line of legality within the Bureau and other organizations authorized, and there would be less use by individual agents of suicide taps or illegal taps.

Would you comment on whether you believe that since the passage of Title III there has been less individual agent initiative in placing, without authority, wiretaps or bugs?

MR. STAFFELD: In the FBI since the enactment of Title III there has been no agent who would at any time initiate a suicide tap in the Title III category.

MR. WESTIN: Do you say that from having an inspection program and a monitoring program that enables you—it is always hard to say that something

hasn't occurred. Law professors like to make a point of the difficulty of proving something did not occur. On what evidence do you say there has been no use by agents?

MR. STAFFELD: I think it is impossible for a single individual to initiate a wiretap or a microphone without having some assistance from two or three or four other people. And you also have to have the cooperation of a telephone company official in order to get a wire to take the sound away from the point at which you are monitoring.

MR. WESTIN: That is a little difficult for me to understand because, given the easy availability of simple devices, either induction coils or miniaturized FM transmitter bugs that can go onto an FM receiver—if you are talking about it simply as opposed to complicated wiretap or bug installations, and recognizing the amount of prosecutions that—I won't mention popular literature that show that private eyes are doing it—I don't see how you can say it would be impossible or next to impossible for an agent to do this.

MR. STAFFELD: All right, let's say it is simple for an agent to install this himself. All of a sudden he comes up with some very sophisticated information. He has to explain where he got it from. And if he can't adequately explain to his supervisor where he got it, he is going to be in trouble.

MR. WESTIN: On the other hand, I think I would assume, from having read quite a number of wiretapping cases, that if you learn some information through an authorized or otherwise tap, the job then is to use it to develop another evidentiary source.

There are any number of ways that you can develop later an independent basis for that. That is, you could tell your supervisor that maybe it would be productive to place a physical surveillance on somebody and the identity of somebody could have come through a wiretap. Or you then suggest that maybe it would be worthwhile to look at the relationship between one holding company and another.

In other words, is it really so difficult for an agent, if he could listen and get useful intelligence on an illegal wiretap, to develop ingeniously, an independent source for the information later in a complex investigation where presumably there was documentary evidence, physical surveillance and a variety of things going on? Would it really be so difficult for him to disguise the source?

MR. STAFFELD: Sir, I am a little bit bothered by the implication. After all, I think each one of us is sworn to uphold the law. And I don't think that in that pursuit an agent is going to become that devi-

ous. I get that import out of it. I don't know if it is intended.

MR. WESTIN: Well, we started off with the assumption—with our agreeing that before Title III there were instances that you knew of, that have been reported—

MR. STAFFELD: This was prior to Title III.

MR. WESTIN: I understand that and I am trying to draw out from you or any others who will comment whether you believe the same kind of zeal to deal with crime and a criminal situation that led those agents to engage in occasional illegal wiretapping before Title III—I am interested in how you are assured today that it is not taking place. I am just trying to understand your statement before that you believe it is not happening. And I wonder what inspection procedures or what other kind of techniques of control you rely on to draw that conclusion.

MR. CLEVELAND: Mr. Westin, we do have a very complete inspection system that looks into all types of allegations against agents. But I think also it should be borne in mind that any special agent of the FBI today who hanky-pankied around with Title III or anything relating to Title III would be doing a disservice to the FBI as a whole and to the country as a whole. Because in Title III we feel we have a very valuable law, and we certainly are going to lean over backwards to try to make certain that we comply with all aspects of that law. And I see no need or justification for any agent of the FBI to do otherwise when actually we have a very good instrument for detecting lawlessness. Why should we play with it?

MR. WESTIN: I take it the import of your statement is you believe that is communicated now down the line so strongly to agents in the Bureau that in no case could any resolution of an individual investigation be as important as preserving Title III authority from the Bureau as a whole.

Is that communicated?

MR. CLEVELAND: I think there is no question about that. I think, on the other hand, that out of any 8,000 given people you may have one bad apple creep in. But I certainly don't know of any instance of that since 1968 when we got the advantage of Title III law. And certainly I think it is pretty well established that anything that goes on in the FBI becomes public knowledge whether it is making an illegal left turn or almost anything else—in book form, the *New York Times*, in the *Washington Post*, or through hearings of this type it will be found out. And since we have heard of none, I think it would follow that there probably have been none.

MR. WESTIN: Well, one way that you try to measure compliance in any agency is the process of investigation of complaint or self-starting inspection. Have there been, since the passage of Title III, any investigations by your office or any other into charges or beliefs that an agent might have been installing a wiretap or planting a bug without having gotten authorization? Has any investigation since 1968 inside the Bureau looked into a charge or investigated some public complaint that might have been brought to the Bureau in that respect?

MR. CLEVELAND: I know of absolutely none in the organized crime field.

MR. KELLY: That isn't a violation that is handled in the Organized Crime Section so we couldn't speak for certainty as to what cases have or haven't been opened. I have a feeling they have investigated them and found they were baseless.

But I do know that as far as organized crime goes, I know of no such allegations that have ever been raised.

MR. WESTIN: Mr. Chairman, have we had any testimony earlier as to whether investigation by the part of the FBI that would have jurisdiction over investigations of alleged illegal activity by agents have taken place since the passage of Title III? I wonder if our Executive Director would know.

MR. HODSON: Mr. Petersen testified about statistics concerning the number of complaints which had been investigated by the FBI, and the number of indictments, I believe, and number of convictions.

MR. WESTIN: I think that deals with other parties.

MR. CLEVELAND: I think you are talking about the interception of communication statute. Mr. Petersen did testify in connection with that. That has to do with violations that we do investigate regularly, yes, sir.

MR. WESTIN: I wonder if we could get them—I understand that you are in the Organized Crime Section. But somewhere in the FBI would there be a unit that would be charged with any inspecting or investigating any allegation that an agent had engaged in illegal wiretapping or illegal bugging? I wonder if we could find out if, since 1968—

MR. CLEVELAND: We will try to find that out for you.

MR. HODSON: Mr. Westin, the first week in June we have scheduled three full days of hearings on illegal wiretapping and I might say the staff has called on the FBI for extensive figures, cases, disposition of complaints, and we will have quite a mass of material to present during those three days which may be the same type of material you are asking these witnesses for.

MR. WESTIN: I don't think so. I am talking about investigation inside the FBI of possible illegal activity by its own agents. I think our June hearings, if I understand them, deal with third-party illegalities or something. But at any rate—

MR. CLEVELAND: We will try to get that for you, Mr. Westin.

[A letter relevant to the above discussion follows.]

WILLIAM V. CLEVELAND

June 12, 1975

General Kenneth Hodson
Executive Director
National Commission For the Review of Federal and State Laws
Relating to Wiretapping and Electronic Surveillance
Room 708
1875 Connecticut Avenue, N.W.
Washington, D.C. 20009

Dear Ken:

By letter dated May 29, 1975, Margery Elfin of your office forwarded a copy of the transcript of the hearings of May 20, 1975, and requested a response to the inquiry of Professor Allan F. Westin, which is contained on page 56 of the transcript.

Professor Westin asked if there had been any FBI investigation since 1968 with respect to allegations of illegal wiretapping or bugging by FBI Agents.

In discussing this matter with the Administrative, Inspection, and General Investigative Divisions of the FBI, there was no recollection of any such investigation. Our Administrative Division has reported that to date there have been no known unauthorized electronic interceptions made by Bureau employees.

Our records management system is designed to permit retrievability of data through a central indices when the specific topic or person constituting the subject matter of interest is known. Under such a system, therefore, it is virtually impossible to categorically state that we have never conducted such an investigation. I can add, however, that in January, 1975, allegations were made which included that Agents of our Houston field office may have engaged in illegal electronic surveillances. This matter prompted an inquiry by the Inspection Division and no information was developed to substantiate this allegation.

It may be of interest to note that the FBI Agents' Handbook specifically states that "employees must not, at any time, engage in criminal, dishonest, immoral, or disgraceful conduct or other conduct prejudicial to the Government." Also, "employee shall not engage in entrapment or the use of any other improper, illegal, or unethical tactics in procuring information or evidence." Further, "no employee should install secret telephone systems or microphones without Bureau authorization."

I trust that the above information will be of assistance to you.

Sincerely,

[Signed] Bill
Assistant Director, Federal Bureau of Investigation

MR. WESTIN: In your testimony you talked about bookmaking operations, gambling, as most susceptible to Title III coverage and the one most devastated by it. Then in the answers you gave to the questions of counsel, you remarked that when

you use the term "bookmaking" you are not talking about the Mom and Pop Shop or the little lady in the candy store, but, rather, large-scale operations.

Subject to many comments that have been made by commentators, if the recommendation were made to take bookmaking out of the jurisdiction of Title III unless it satisfied certain criteria as to scale or as to relationship with organized crime, that is, if you were required by amendment of the statute to make a showing before a Federal judge that what is called bookmaking and policy operation meet certain minimal criteria, that you had to demonstrate that in the probable cause process, would that be acceptable to you or do you think that would be a problem?

I am trying to square, in other words, your own rules with something our Commission might recommend to be built in as an amendment. Because I think a lot of people when they read this language and didn't hear you—when various commentators have read it they have leaped on the idea of bookmaking and said "Why have this when even the dogs in the street know who the bookmakers are?"

MR. CLEVELAND: I don't think that would be a problem, Mr. Westin. We have a situation now where the United States Attorney or the Strike Force will not authorize prosecution in connection with the case unless there are certain criteria present.

Some, for example, insist that members of a syndicate be involved before they will authorize prosecution.

Others will insist that either a member of the syndicate or corruption is shown in connection with the operation.

The difficulty, however, in a recommendation that this be across the board is the fact that what is a major operation in New York City would not necessarily be the same criteria of a major operation in Mobile, Alabama, if you follow me.

And this not only applies to gambling, but this applies to all types of Federal crimes. The theft and interstate transportation of an automobile in New York City is not considered the same type of violation that it might be in the South or Southwest, you see.

So, really, to make a recommendation of that type across the board would be fairly difficult, I believe and, as a matter of fact, in handling quality-type cases rather than quantity we have found that we've got to more or less follow the edicts of the individual United States Attorneys throughout the country as to what they feel is a quality case rather than to define a quality case across the board because it changes from jurisdiction to jurisdiction.

MR. WESTIN: I appreciate that as a matter of difference by location and type of community—

MR. CLEVELAND: Right; right.

MR. WESTIN: —on the other hand, the way you have described it, it puts the essential decision in the hands of the United States Attorney or your office with the United States Attorney. It doesn't identify that as a criterion that the courts should be looking at.

I wondered if there was some way in your mind that you could see a definition of what was clearly outside the scope of Title III wiretapping and bookmaking and policy operation with some standard of relevant size based on the community or the type of setting that the courts, in effect, would be policing.

Because it seems to me one of our concerns is: What should the role of the judiciary be? What are the standards of probable cause under Title III and how do you make them clear enough so the Federal judges understand their role, for example?

Do you think this is in essence beyond the competence of the Federal judge to pass on or do you see that the Federal judge should be given a determinate role here?

MR. CLEVELAND: Again I think it is a difficult thing to say nationwide that XYZ will be the criteria to follow. Because I think that the United States Attorneys and the judges throughout the country feel that they have an obligation to take care of the local situation existing in their particular areas. And for that reason, their criteria are going to change from locality to locality as to what they consider to be a quality-type case or a serious-type crime.

PROFESSOR BLAKEY: Alan, may I ask a follow-up question?

Maybe I should really ask Mr. Staffeld this.

Do you have available to you at the point of seeking the wiretap sufficient information to know what quality the case is going to be when you finish the tap?

I could see limiting the prosecution to quality cases, but I am really asking: Could we develop a pre-use standard for when Title III should be used to guarantee it is only used in quality cases? Isn't whether it is a quality case often something that is determined after the tap and not before? I am concerned that if you put on very sophisticated criteria to limit the use of wiretapping to quality cases, it might destroy the tool. Isn't the reason you are using the wiretap to find out if it is a quality case?

MR. STAFFELD: No, I don't think that is true. I think when we get to the point of inserting the Title III in the investigation, finding it is necessary, we have at that point a very good idea of the volume—and this is based on informant information—and the nature of the network, the size of the network, and what these individual runners might be handling.

I think it would be very unfortunate to attempt to codify the type of a case that we should be in or we should not be in.

In other words, if you say that we can investigate and prosecute only those wherein there is an annual handle of a million dollars, aren't we in effect saying that that fellow that is operating on three-quarters of a million dollars is legal? And I would hate to see that position.

CHAIRMAN ERICKSON: Do you have any further questions? If not, we will take a recess.

[Whereupon, a short recess was taken.]

CHAIRMAN ERICKSON: May we reconvene.

First, Mr. Cleveland, I understand there is a brief clarifying statement that you would like to offer the Commission.

MR. CLEVELAND: Yes, Judge, thank you very much.

In connection with one of your questions, Mr. Westin, apparently someone got the impression that I was not opposed to setting specific criteria in connection with quality-type gambling investigations. I would like to correct that impression, if I did convey that.

I pointed out that some Strike Forces will not authorize prosecution unless there are one or two elements present. We don't necessarily feel that this is a correct procedure. If there is a quality-type case and we have investigated that case, we think it should go through the prosecutive processes.

I also pointed out that in different areas you have different criteria followed in connection with gambling-type investigations. So, therefore, it would be most difficult for an across-the-board criterion to be spelled out as to what gambling cases should be prosecuted and what gambling cases should not be.

So if there is any misunderstanding that I am in favor of criteria of that sort, I would like to correct that now and answer any further questions you have on it.

MR. WESTIN: Does that mean if you get into a small community where something that would be a Mom and Pop operation in New York is regarded locally in a rural or suburban community or a small city as being a significant one, then in that case you would say that it would be all right to put in a Title III, even though it falls, if not in a Mom and Pop, at least in a small-scale operation?

MR. CLEVELAND: Absolutely. For example, we have had cases in southern cities where those cities feel that they have a real problem with a numbers-writing operation, and we have gone ahead with the case with the United States Attorney's authority and have broken up that operation through investigation, through use of Title III, and prosecutions have followed.

In New York and other major cities they may not touch such an operation as that, but in the South they feel it is important that it be disrupted.

Does that answer it?

MR. WESTIN: Yes.

MR. CLEVELAND: All right, sir.

PROFESSOR BLAKEY: Mr. Chairman, I just want to ask one more question.

CHAIRMAN ERICKSON: All right.

PROFESSOR BLAKEY: I think I didn't really make my question clear, Mr. Staffeld.

What I was worried about goes something like this: there are various kinds of people in the criminal justice process making various kinds of decisions. What Congress has done in Title III is formulated legal rules governing when to put in a wiretap. They have done this using, among other things, crime labels. They have set a standard saying, "probable cause that a crime has been or is going to be committed." They have then asked you to make an evidentiary showing under the probable cause standard. They have asked you to make it to the judge.

That is the traditional way investigations are limited.

I understood what Professor Westin was getting at was a different kind of decision. He was referring to the investigative decision to use tapping, or the prosecutive decision to bring a case, that is, when a case was "appropriate." He was asking whether you thought that this concept could be formulated in something like a legal rule and whether then you could make factual showings to meet that legal standard and make it now, not inside the agency and your investigative process, but in court, through affidavits, and ultimately be willing to, I take it, have that "investigative decision"—not "probable cause decision"—be reviewed by defense counsel on a motion to suppress and by appellate judges later on.

Does the investigative process lend itself to the formulation of standards and then to the establishment of those standards before a judge?

MR. STAFFELD: Well, I think I indicated that we do sometimes have some knowledge of the extent or the volume of the gambling operation.

Now, this is only a guideline, an investigative guideline. It certainly is not evidence and we certainly could not go into a court and establish at the time we submit our Title III that this outfit does in fact handle \$10 million a year. We certainly wouldn't want anything like that. It would be totally impossible for us to work.

PROFESSOR BLAKEY: While you might be able to have informant information that a person is a member of LCN—

MR. STAFFELD: Same thing.

PROFESSOR BLAKEY: If you got beyond LCN, which is a kind of established group—it actually has formal membership—do you think you could formulate an investigative definition of organized crime and then prove it in an application for a wiretap?

MR. STAFFELD: There are dozens of definitions of organized crime and I think that to establish any one from the standpoint of meeting the needs before you undertook a Title III would be totally impossible.

PROFESSOR BLAKEY: In other words, the statute just wouldn't work.

MR. STAFFELD: It wouldn't work; it wouldn't work. And I don't think—after all, we talk about LCN. They don't have membership cards. How would you establish membership? It couldn't be done.

CHAIRMAN ERICKSON: Mr. Pierce.

MR. PIERCE: I have no questions.

CHAIRMAN ERICKSON: Judge Shientag.

MS. SHIENTAG: I really shouldn't take the time of the Commission to ask the question, but I can't help but, when we have this august body, you, Assistant Director Cleveland and your cohorts, to try to pursue this line of questioning which Professor Blakey started on.

You have had all these investigations since, in my time, Kefauver. We have in this body been spending money interviewing witnesses, taking your men from the field to testify and help us find out whether wiretapping and electronic surveillance is an important weapon in the arsenal against crime.

Yesterday the *Washington Post* said that \$14.5 billion are spent in combating crime, and where are we? We have more crime than ever.

Well, in addition to the Title III authority that is given, is there anything else that you, in your wildest dreams, could conceive of as helping, as a weapon, to combat crime? Is there some other way within the Constitution that would help us to get at the LCN and the others who don't provide membership cards?

MR. CLEVELAND: That is pretty difficult to answer. As you have already stated, considerable manpower and funds have been thrown into the effort to try to go into all of them, because I am sure you have heard them from others who have testified here.

The main thing we would hope to do, however, is to bring about some type of control to the increasing spread of crime, not only from an organized crime standpoint—

MS. SHIENTAG: Is there anything in trial rather than investigative procedures that would be helpful?

MR. CLEVELAND: Well, of course all investigators feel that the judge should hand out more sentences more speedily.

MS. SHIENTAG: Do you feel that higher sentences, lack of plea bargaining, or methods of that sort would be helpful in keeping the people whom you have investigated out of the realm of crime?

MR. CLEVELAND: Well, I think personally that there is nothing that is a bigger deterrent to crime than speedy justice and jail time. And I am afraid that we don't have either one to any great extent these days.

Many people that are arrested in connection with serious crimes are back on the street the next day. Their cases may or may not come up within the next year or two. And through plea bargaining they may never see the inside of a jail.

I don't think that that is a great deterrent to additional crime.

I do think speedy trials and some jail time does amount to a deterrent to crime.

MS. SHIENTAG: Thank you. I agree with you.

CHAIRMAN ERICKSON: Is that all, Judge?

MS. SHIENTAG: Thank you.

CHAIRMAN ERICKSON: Mr. Remington.

MR. REMINGTON: I have no questions.

CHAIRMAN ERICKSON: Chief Andersen.

CHIEF ANDERSEN: I have a couple of questions.

On the State level, wiretapping authority rests with the District Attorney, in most cases. On the Federal level, however, it stays with the Attorney General in Washington. If a recommendation were made, suggesting that this final authorization for a Title III be given to the United States Attorneys, what effect would that have on your review process and on the Bureau?

MR. CLEVELAND: Chief Andersen, it would have the effect, I believe, of possibly tending to liberalize the stringent rules that are presently in effect on Title III, and we feel that the stringent rules now in effect are quite important to maintain.

To say it another way, Chief, if they remove from the Attorney General the approval process of Title III's and moved it to the United States Attorney level, as I believe you said—

CHIEF ANDERSEN: Yes, that is what I said.

MR. CLEVELAND: —I think that would have a tendency to give people the idea that we are not giving the amount of time and attention to these things that we should be giving them to make certain that we are not invading privacy or taking advantage of the act which we feel is so valuable in our investigations.

I think it is perfectly well established now that we should have a good, thorough review of each and

every request for a Title III throughout all the steps that they now take all the way to the Attorney General, and then out to the judge and even at the judge level we now have questions.

I could give you a couple of examples. We had one judge in Pennsylvania, for example, that sat down with an agent on an affidavit for a period of three hours and went over each word of the affidavit to satisfy himself that we had everything in there that should be in there before he authorized the installation.

We had another judge recently in the Midwest who was not satisfied with the fact that the Attorney General had authorized a particular installation. He wanted additional assurances from the Attorney General that before he went ahead with the authorization he was absolutely within the law.

So from that standpoint, I believe it is important that we maintain the very careful scrutiny Title III's are given today.

CHIEF ANDERSEN: So you would see a danger to that at the Washington level of the possibility of—I won't use the word "abuse," but something like that?

MR. CLEVELAND: I think there would be the danger that people would feel there would be a lessening of the thorough degree of review that they are presently given. I do think that.

CHIEF ANDERSEN: We have been hearing testimony from Strike Forces which are a whole new concept, of course, in Federal law enforcement, and I am getting the impression from listening to people on Strike Forces that practically all Title III's in cities that have Strike Forces are coming from the Strike Forces rather than from the other agencies. Is that a practice we are falling into? Or am I wrong?

MR. CLEVELAND: Well, there are 17 Strike Forces, Chief—actually 15 different cities involved, because there are two Strike Forces in New York and there is a 17th one here at Headquarters handling specialized matters. So you have 15 major cities involved.

Were they not there, the same degree of closeness would exist between the United States Attorney and the investigating agency insofar as Title III's are concerned. Simply because there is a Strike Force in Kansas City or another city means we work closely with them in establishing probable cause and preparing the Title III affidavit, and we also work closely with them in the actual installation, keeping them advised daily of what is transpiring over that particular coverage, so it can be discontinued the minute there is sufficient evidence in their opinion to go ahead with prosecution.

MR. STAFFELD: I think the point is, Chief, that Strike Forces are organized for the purpose of pursuing organized crime. And this is the channel or this is the area in which the Title III is used most frequently. And, as a consequence, it falls within the category of the Strike Force to pursue.

MR. KELLY: Also, Chief, by virtue of the fact they are in the principal cities where they believe organized crime is more prevalent, it stands to reason these would be the people who would process more applications in this field.

CHIEF ANDERSEN: But I find a conflict in review process between the Strike Force and regular agencies. Who reviews Title III applications for Strike Forces at the Washington level?

MR. CLEVELAND: The Organized Crime and Racketeering Section of the Department of Justice, which is part of the Criminal Division—

CHIEF ANDERSEN: Of the Justice Department?

MR. CLEVELAND: —of the United States Justice Department—reviews the affidavit and they are usually reviewing it at the same time we are reviewing it at the Headquarters level.

MR. KELLY: Chief, if I could clarify this a little, the same review process takes place whether the request comes from a United States Attorney or a Strike Force. The same review process would take place at Bureau Headquarters and the Department.

CHIEF ANDERSEN: It comes through the Federal Bureau of Investigation. All right. And if it is a drug case—

MR. CLEVELAND: —it would go through the DEA.

CHIEF ANDERSEN: I have been a little confused on that, thank you.

CHAIRMAN ERICKSON: Just a few questions, Mr. Cleveland.

First, Mr. Westin was asking about different standards of the FBI relating to the Mom and Pop operation in a small community against the LCN operation in, say, New York City or some other major area.

Regardless of where the information comes from that leads to the production of an affidavit and the application for a wiretap, it receives the same review, does it not?

MR. CLEVELAND: It receives exactly the same review.

CHAIRMAN ERICKSON: What?

MR. CLEVELAND: The decision is different.

CHAIRMAN ERICKSON: But if a tap is to be issued in accordance with Title III, it would still have to meet the same tests?

MR. CLEVELAND: Exactly.

CHAIRMAN ERICKSON: So, as far as having different standards is our concern, there is no dif-

ferent standard. Probable cause is probable cause regardless of how you cut it; isn't that true?

MR. CLEVELAND: And the review procedures would be exactly the same.

CHAIRMAN ERICKSON: So you are not giving one brand of justice in South Carolina and a different brand of justice in New York City?

MR. CLEVELAND: No, sir.

CHAIRMAN ERICKSON: As far as the exhaustion of procedures test is concerned, that is explored in connection with the use of Title III, is it not?

MR. CLEVELAND: I'm sorry. I didn't catch the first part of your question.

CHAIRMAN ERICKSON: Before you undertake to seek the right to install a wiretap pursuant to the provisions of Title III, all other investigative procedures are exhausted, isn't that true?

MR. CLEVELAND: That is correct.

CHAIRMAN ERICKSON: And that is passed upon by the Department of Justice or by the FBI?

MR. CLEVELAND: By the FBI and the Strike Force or the United States Attorney, yes, sir.

CHAIRMAN ERICKSON: So it is not done in every case?

MR. CLEVELAND: No.

MR. STAFFELD: We attest to the fact in the affidavit that all other procedures have been tried.

CHAIRMAN ERICKSON: Oh, I understand that, but one of the problems that we have had to face is many of the affidavits are what have been referred to as boilerplate as far as certain allegations are concerned. And I am trying to ascertain if it isn't really boilerplate, but rather that this is examined to determine whether or not other procedures have been followed.

It is not anything that is passed upon lightly.

MR. STAFFELD: Not a bit.

CHAIRMAN ERICKSON: In the use of these Title III intercepts, they are used to a large extent on organized crime?

MR. CLEVELAND: Yes, sir.

CHAIRMAN ERICKSON: And organized crime isn't always productive as a rule?

MR. CLEVELAND: That is right.

CHAIRMAN ERICKSON: And, as a matter of fact, it is suggested that in some instances there might be a conspiracy between some of the individuals that operate?

MR. CLEVELAND: Exactly right.

CHAIRMAN ERICKSON: So the conspiracy that would be the subject of the investigation would not be one that you could determine the limits of by ordinary investigative techniques just by the nature of the beast, isn't that true?

MR. CLEVELAND: That is true.

CHAIRMAN ERICKSON: In using this procedure that is outlined by Title III, rather rigid standards were established in 1968, when the law came into being, which permitted the use of the evidence that you obtained by intercepts using electronic means?

MR. CLEVELAND: Yes.

CHAIRMAN ERICKSON: Prior to that time you had interpreted the Federal Communications Act and Section 605 to deal with interception and divulgence; isn't that true?

MR. CLEVELAND: Yes, that is true.

CHAIRMAN ERICKSON: And so, prior to that time, you were not restricted as much as you are now as far as the interception is concerned.

MR. CLEVELAND: I think that would probably be true, as far as the interception is concerned.

CHAIRMAN ERICKSON: Yes. You were free to make broad interceptions under your interpretation of the Federal Communications Act, Section 605, but you couldn't use the evidence.

MR. CLEVELAND: That is true.

CHAIRMAN ERICKSON: So if you found something that was probative, relevant, material and convictorial, you had to hope that you could establish this by another means?

MR. CLEVELAND: That is right.

CHAIRMAN ERICKSON: So the invasion of privacy was greater prior to the passage of the Title III provisions? In short, privacy rights, whether it be of organized crime or Mom and Pop are greater now than they were before the passage of the Act?

MR. CLEVELAND: I think that is true.

CHAIRMAN ERICKSON: And the time and the protective measures are greater now?

MR. CLEVELAND: Yes.

CHAIRMAN ERICKSON: Now, you have testified that the safeguards are satisfactory as they now exist to protect the needs of law enforcement while protecting privacy. But the questions which Chief Andersen propounded and which have come about as focal points in the testimony of some other witnesses, would indicate that this Act could be improved upon without violating rights of privacy and to provide for some simplification, such as having less of a chain of review.

As I understand it, you feel at this time that such changes are not required.

MR. CLEVELAND: That is correct, Mr. Chairman, and I think it has been brought out very well here this morning why I feel that way. As long as we have Mr. Westin and others who feel we are violating some of the precepts of the Title III law, I think it is very well that we have very stringent rules governing our conduct in connection with this fine act.

CHAIRMAN ERICKSON: Those are all the questions I have.

Mr. Cleveland, we are indebted to you and the Department of Justice and the Federal Bureau of Investigation for the cooperation you have shown.

Thank you very much, Mr. Cleveland.

We will now take the testimony of Mr. Robert Sweeney, Special Agent and Supervisor, Organized Crime Division.

And we again thank you, Mr. Cleveland and I hope that we will see you again soon.

And, before you leave, I might tell you that when I left to accept the phone call, the person that called me was Congressman Butler and he apologized for not being here and said he was extending the apologies of the other Congressional members who had hoped to be here to hear your testimony, but that there was a quorum call on a matter of some urgency that prevented him from being here.

Mr. Sweeney, you have already been sworn and I understand that you do not have a prepared statement but that you do have a summary that you would like to make to the Commission before interrogation is commenced.

**TESTIMONY OF ROBERT SWEENEY,
SUPERVISOR, ORGANIZED CRIME
DIVISION, FEDERAL BUREAU OF
INVESTIGATION, NEW YORK CITY,
ACCOMPANIED BY ALVIN A
STAFFELD, INSPECTOR, AND JOHN E.
KELLY, JR., INSPECTOR, FEDERAL
BUREAU OF INVESTIGATION**

MR. SWEENEY: No, sir, really I am prepared right now to respond to any questions concerning my activities with Title III.

CHAIRMAN ERICKSON: You don't have a statement that you would like to make at this time?

MR. SWEENEY: No, I don't.

CHAIRMAN ERICKSON: All right. Following our usual procedure, Mr. Cook of the staff will interrogate you first.

MR. COOK: Mr. Sweeney, can you tell the Commission what your present position is?

MR. SWEENEY: Yes. I am a Supervisor in the Organized Crime Division and have a designation of the Number One Assistant to the Agent in Charge of the Organized Crime Division in New York.

MR. COOK: And how long have you been in New York City?

MR. SWEENEY: Oh, approximately 21 years.

MR. COOK: And you did have experience as Supervisor of the Hijacking Squad?

MR. SWEENEY: Yes, I worked Hijacking and supervised that squad for a number of years.

MR. COOK: Can you tell the Commission, relating to your activities as Supervisor of the Hijacking Squad, what is ordinarily involved in the commission of hijacking on a commercial scale in New York? Can you tell us what a typical operation would be like?

MR. SWEENEY: Yes. Hijacking in New York, of course, was quite prevalent during the time I had the Squad. I think those were considered the peak years as far as numbers of hijackings. There were approximately one every work day, say 20 a month at that time. They had no dollar-and-cent figure as to what the thefts were.

However, there were two types. One was where two or three individuals would accost a driver at a stoplight or wherever and at gunpoint take the truck away from him and put him in the trunk of a car and hide him out for a period of an hour or two until the truck had been either concealed in a garage or they unloaded the stolen contraband and he was released usually unharmed. Very few times was he ever harmed, to my recollection.

And the standard theft from the street would be a truck parked on the street, say, in the garment area of New York City. The driver would leave to make a delivery and when he came back of course the truck was gone and so was all the cargo on board. The empty truck would be found abandoned in some rather remote area of New York City.

MR. COOK: Was there a particularly high incidence of hijacking in the waterfront areas and the Port of New York?

MR. SWEENEY: No, I would say, while there were a number of hijackings in the waterfront area, I would say the garment area was probably the leader, if you can call it that, as far as numbers of hijackings.

MR. COOK: And what were the principal goods that would be stolen in hijacking offenses?

MR. SWEENEY: Well, New York, of course, being a large city, anything that could be fenced. But piece goods is definitely a leader. Cigarettes, when available; liquor when available—any of the high-commodity items—television sets—anything that would sell. And piece goods, of course, is one of the big items in the garment area and there were many thefts in that field.

MR. COOK: Would you tell us what piece goods is?

MR. SWEENEY: Piece goods is the unfinished fabric or the finished fabric. It comes in a large roll. It approximates, I would say, a 20-foot straight job, as they would call it—you might have a 40 or 50 thousand dollar load of piece goods. It is the

material before it is made into a garment, finished or unfinished. Unfinished would go to a processing plant to be processed into clothing. It is extremely valuable and hard to identify and can be marketed easily in New York City.

MR. COOK: Who composes the market for stolen goods? Legitimate people who buy the stolen goods unwittingly?

MR. SWEENEY: I don't think too many people buy it unwittingly, but it is being plowed back through individuals who are willing to buy and fence, and certainly it can be sold legitimately in the final analysis. But prior to that, I would say most of it is an illegal type of buy in the buying situation.

MR. COOK: During the time when you were Supervisor of the Hijacking Squad were you made aware of or a participant in the intelligence-gathering activities which would indicate the existence of organized crime families in New York?

MR. SWEENEY: Well, organized crime families and hijacking have been closely allied in New York City. I don't think there is any doubt about that. In the popular phraseology, the hijacker of today would be the organized crime figure tomorrow, and there are a number of very major organized crime figures in New York City who started out—their first arrest would be for hijacking or they are in jail now for hijacking. One leader, a very strong individual in New York City, is now serving time for a hijacking he committed in 1959. I think it was almost ten years before he was finally convicted of the crime. But this is a typical history in New York City.

MR. COOK: And when you were supervising the Hijacking Squad, did you have any liaison with the organized crime investigating authority?

First, let me ask you, what was the composition of the Organized Crime Squad during the tenure of your supervising the Hijacking Squad?

MR. SWEENEY: It was relatively the same as it is now. The Hijacking Squad has always been closely allied to the organized crime field, either part of the Division or working very closely with the Organized Crime Division.

MR. COOK: Is there any particular element in the hijacking industry, if you can call it that, that indicates to you that organized crime is involved?

MR. SWEENEY: Well, we know from our intelligence sources that certain organized crime figures have been operating with what they call a crew, and they have crews that are involved in stocks and bonds, for instance, or they will have a hijacking crew. I don't mean that the actual organized crime figure himself, that is, a legitimate member, is out hijacking. But this could easily be his operation. The fence or whatever is feeding back to him.

And occasionally we will involve some organized crime members in a hijacking or the fencing or the buying or possession of stolen property.

MR. COOK: So there is very little doubt that a substantial amount or at least a significant amount of the properties from hijacking goes to the coffers of organized crime?

MR. SWEENEY: I believe so; yes, sir.

MR. COOK: Now, has there been any significant use of electronic surveillance in the area of hijacking or theft in New York City?

MR. SWEENEY: No, sir.

MR. COOK: And are there any particular reasons for that?

MR. SWEENEY: Well, there are several reasons, I would say. One is the development of probable cause. We would have to show that the particular phone or location where we are attempting to install electronic coverage would be used for, say, the discussion, the planning, the conspiracy of hijackings and the theft from interstate shipment. In other words, our statutes have an interstate aspect to it, either that the cargo is moved in interstate commerce or the fact that after it is stolen it is going to be moved, before we would have jurisdiction. That is one thing probable cause is difficult to develop on under the statutes.

The second thing is I would be on, say, a given location, the planning of it—a room or a loft or what have you—say there would be a 20-day or 15-day Title III, there is no guarantee in there that during that 15 or 20 days there is going to be a hijacking discussed. In other words, hijacking is not like gambling where it is a day-to-day wire room. They move when they have an opportunity or whenever the mood suits them or whatever stimulates their activity in the hijacking field. It is not a day-to-day operation. It is a field that I would say we are very interested in. We have looked at it closely. We have had some Title III coverage in that field and we anticipate that possibly in the future we are going to have more. We have not had what we would desire at this point.

MR. COOK: Have you had any success at all in Title III investigations in the hijacking field, or fencing?

MR. SWEENEY: I don't know of any hijacking convictions we have as a result of Title III.

MR. COOK: And by conventional means is there any significant number of hijacking convictions in New York?

MR. SWEENEY: Yes. I would say one of the greatest number of convictions probably in the New York office would come as a result of our investigation in the hijacking field.

It is most certainly one of the crimes we are most successful in combating as far as the number of arrests and convictions is concerned.

MR. COOK: What particular techniques account for your success in this field? Is it search and seizure?

MR. SWEENEY: Well, any law enforcement agency is—we are operating on information received. In the hijacking field it would be the development of live informants, our own observations and surveillance activities on a known what they call a drop or known figures in the hijacking field. And certainly we are able, in a sense, to categorize certain individuals in New York City as to what they handle, whether it is furs, cigarettes, liquor, or what have you—not that they are that specialized, but there are certain people who specialize in piece goods. That is definitely a specialized field.

MR. COOK: And in your operations, you are the Number One Man in the Organized Crime Squad. Do you have occasion to deal in the gathering of intelligence?

MR. SWEENEY: Yes.

MR. COOK: What are the principal modes of intelligence gathering the New York Office uses at this time?

MR. SWEENEY: Well, certainly the principal mode of intelligence gathering would be informant coverage, and whatever we have from Title III and whatever we have through observation. Observation, of course, is limited. We can see that two or three organized crime figures are meeting some place, but we certainly don't know what they are saying or what they are doing. I think we passed long ago the idea that it was of great significance to observe a half-dozen LCN figures, say, sitting some place if we don't know what they are talking about. And I am sure they are well aware of it, also.

MR. COOK: As a result of the intelligence gathering carried on in New York City in the last five or ten years, you have been able to establish the existence of various organized crime groups; isn't that right?

MR. SWEENEY: Yes, we have.

MR. COOK: Have you been able to identify particular individuals within these groups who are active in specific areas of criminal activity?

MR. SWEENEY: Yes, we have.

MR. COOK: And is it fair to characterize this as "targeting"?

MR. SWEENEY: Yes, definitely.

MR. COOK: Now, once you have targeted an individual as being active in organized crime, what limits do you place on the means that you will employ in an attempt to secure convictions against that person?

MR. SWEENEY: Well, at the moment probably our only limitation would be legality, if that is the course you are taking. We at the moment are not suffering any manpower problems. I mean we have sufficient manpower, we believe, to do what we are doing. Naturally we could always use more, but it is an all-out investigation.

I might explain that in the organized crime field we generally work the case backwards, contrary to another investigation. We have an organized crime figure. Now we are trying to find out what he is doing. We know he is doing something illegal. We know he is profiting by his illegal activity. We are trying to find out what it is and arrest and convict him of the crime. It is not like a bank robbery where somebody walks in and robs a bank and we are trying to find out who did it.

In this case we know the individual and are trying to find out what he has done and prove it in court. So it is a backward procedure in some respects.

MR. COOK: In the course of focusing your investigative attention on a given individual, do you assign specific agents to cover that person?

MR. SWEENEY: Yes, we do. In the target areas we will have an agreement as to, say, a key target or somebody we are interested in. And certain agents from a certain squad acting under their supervisor will be designated to work, say, this individual.

MR. COOK: Now, is there any way in which you can tie your electronic surveillance activities into informants?

MR. SWEENEY: Definitely. One of the greatest tools we have in finding out—not finding out but getting him convicted of what he is doing, is Title III. For instance, our informants can possibly tell us that a certain individual has a large-scale gambling operation in New York City. We know this. To develop a prosecutable case against him we need a weapon such as Title III to establish evidence.

MR. COOK: Now, according to an article I read recently in the *New York Times* that went into some detail, the New York office used what I thought was a fairly innovative and imaginative approach to electronic surveillance investigation—and I am referring now to the establishment of the Whalen Coat Company.

Can you describe to the Commission the method by which this operation was conceived and the types of things you hoped to gain by it?

MR. SWEENEY: Mr. Cook, I think I would have to decline on that. The Whalen Coat Company is still under prosecution. It has not been adjudicated by the courts so I would rather not.

I can comment in a general way on undercover projects of this type, I think.

MR. COOK: Okay.

If we can deal in hypotheticals, then, as part of your general program, I take it the existence of the Whalen Coat Company case indicates that you had made a decision to take affirmative, aggressive steps in establishing contacts inside the organized crime community?

MR. SWEENEY: Yes.

MR. COOK: And this was in the garment district?

MR. SWEENEY: Yes.

MR. COOK: And what types of indications did you have that made you feel that this type of operation would be successful—in a general way?

MR. SWEENEY: Well, I would say in a very general way—and certainly the garment area of New York City, I think, is a target that has attracted all of law enforcement in New York City for years. It is a common saying in New York, "If it exists in New York City, it is in the garment area." We have almost every crime known to us being committed there. So penetration of the garment area has not through the years been successful. People are unwilling to testify. Loansharking in some respects is a way of life there. There are certain reasons the garment area could never be penetrated.

This is why we felt, along with the others who participated in projects of this type, that something unusual in the way of an investigative technique had to be developed.

MR. COOK: Have you had any occasion in developing these new techniques to employ the statute dealing with Racketeer Influenced and Corrupt Organizations, the so-called RICO statute?

MR. SWEENEY: Yes, we have.

MR. COOK: Without disclosing any existing investigations, have you been able to conceive of situations in which you might utilize surveillance in RICO investigations?

MR. SWEENEY: Yes, we have.

MR. COOK: When you target someone, you assume that certain measures, investigative measures, are going to be necessary to secure a conviction against that person?

MR. SWEENEY: That is correct.

MR. COOK: One of the requirements which everyone is quite familiar with in determining if a Title III may be used in an investigation is that normal investigative procedures be exhausted. Implicit in your targeting of someone is the conclusion that normal investigative procedures will not succeed against this individual?

MR. SWEENEY: I would not say that is true, no. We bring down a number of cases by search warrants—gambling operations—without the use of a Title III. We don't start with the basis that we are going to have to have a Title III before this is over.

MR. COOK: I see.

MR. SWEENEY: Am I making myself clear?

MR. COOK: Yes; go ahead.

MR. SWEENEY: That basically is it. In other words, when we start an investigation on an organized crime figure there is no reason—we might, in the back of our minds, have the possibility, but certainly we don't start out with the idea before we make an arrest or conviction that we are going to have to have a Title III.

I think possibly if people could understand the amount of work that goes into a Title III, they would realize that all other investigative effort has been exhausted prior to us entering into it, because just on the manpower alone we burn up a tremendous amount of manpower. It is a very difficult procedure.

MR. COOK: I see.

Can you give the Commission any specific citations, in terms of closed cases or convictions, where your targeting has been successful in disrupting an ongoing criminal organization?

MR. SWEENEY: I would say that certainly as to one family in New York we feel that we have disrupted, splintered, decimated—put them in a bad way, so to speak. And it mainly came about as a Title III. I often feel if we had done as well against all others as we had against this one particular group, we might be out of business.

But as a result of the Title III primarily, we were able—this is just an example—to do a great job at disrupting one family completely.

MR. COOK: What family was this?

MR. SWEENEY: Columbo.

MR. COOK: You indicated that it would be your desire to be as successful against the other four organizations or families. Were there any particular aspects of the Columbo investigation which indicated to you you might have success against some of the other families by using some of the same techniques?

MR. SWEENEY: Well, yes, I would say that it certainly pointed the way as to what could be done in other organized crime groups.

MR. COOK: I see.

Mr. Chairman, that concludes the staff's questions.

CHAIRMAN ERICKSON: Thank you very much, Mr. Cook.

Professor Remington.

PROFESSOR REMINGTON: I have no questions.

CHAIRMAN ERICKSON: Chief Andersen.

CHIEF ANDERSEN: Just a couple of questions.

Do you cooperate on state wiretaps up there? Is this a cooperative group?

MR. SWEENEY: The Southern District of New York has a joint Strike Force where the New York City police, the State police, and all is a member and we have cooperated in major investigations with almost every investigative body there, yes.

CHIEF ANDERSEN: So even in the hijacking in these areas you do use State of New York Title III's?

MR. SWEENEY: No, we don't. No, our Title III's have generally been our own. As far as hijacking is concerned, the city—it is not really a state problem. It certainly is a New York City problem, because most of the thefts occur in the confines of the city.

But as far as a Title III with them on a matter such as hijacking, no, sir.

CHIEF ANDERSEN: I am trying to find out if the Federal agencies are using State wiretaps rather than going through the 21-day review process at the Justice Department.

MR. SWEENEY: No, sir, we are not.

CHIEF ANDERSEN: And I am not saying it with any maliciousness, but just for ease of operation.

MR. SWEENEY: No.

CHIEF ANDERSEN: We have had testimony where it seems they are using the State statute and that is why I am asking.

MR. SWEENEY: No, sir, we haven't had that experience.

CHAIRMAN ERICKSON: Mr. Pierce.

MR. PIERCE: Has the number of families in New York increased, decreased, or remained the same over the last 30 years?

MR. SWEENEY: I would say remained the same, I guess—maybe not for 30 years but for a number of years.

MR. PIERCE: Same names and everything?

MR. SWEENEY: The names have changed. I think you will find that it is popular among law enforcement agencies to refer to them by old names although the leaders were deceased, because they were the last extremely strong figure to lead such a group.

MR. PIERCE: Do you think the FBI and the other law enforcement agencies operating in New York have succeeded in decreasing organized crime in New York in the last 30 years?

MR. SWEENEY: I think that we have definitely taken steps towards decreasing organized crime. Again, I wouldn't say—I couldn't tell percentagewise or numberwise, but we certainly have had some great deal of impact on organized crime in New York City.

MR. PIERCE: But if the families remain the same in number, are their profits the same, or more?

MR. SWEENEY: Their profits I would have no way of knowing. I would say that their

number—they certainly haven't spread and they have probably decreased numberwise.

MR. PIERCE: Are they in the same kind of crime as they were 30 years ago?

MR. SWEENEY: Well, I think that there is a popular myth that organized crime is in certain fields and not in other fields. Organized crime generally is in any field where there is money to be made. They will even go quasi-legitimate if they can make money at it.

MR. PIERCE: They have been going quite quasi-legitimate in recent years, have they not?

MR. SWEENEY: Yes. There is no doubt about it as far as my personal opinion is concerned, wherever there is a possibility to make money you can find elements of organized crime showing an interest.

MR. PIERCE: And they have been doing the same thing over the past 30 years?

MR. SWEENEY: Generally.

MR. PIERCE: Thank you.

CHAIRMAN ERICKSON: Judge Shientag.

MS. SHIENTAG: Mr. Sweeney, the hijacking that you talk of in the trucking industry, in the garment industry, is that involved with extortion in trucking? Is that similar to the operation that some 40 years ago Lepke and Guerra had—the same type of thing?

MR. SWEENEY: The old shake-down extortion?

MS. SHIENTAG: Yes.

MR. SWEENEY: No, it is a different situation whatever. The hijacking in New York, as I described it, is actually placing a gun at the head of the driver.

MS. SHIENTAG: But in addition to the hijacking there is an extortion—I don't think it is a labor extortion, but it involves the trucking industry—going on now in New York. Are you familiar with it?

MR. SWEENEY: Yes.

MS. SHIENTAG: It has been in the newspapers and is public knowledge.

MR. SWEENEY: Yes.

MS. SHIENTAG: Is that one of the things under your jurisdiction?

MR. SWEENEY: We are interested in it and it comes under our jurisdiction, a great deal of it. We are interested in it from the organized crime standpoint.

MS. SHIENTAG: Are you working in collaboration with any other agency?

MR. SWEENEY: In many instances the Joint Strike Force of New York is our immediate partner.

MS. SHIENTAG: Specifically with the target of the extortion in the trucking industry?

MR. SWEENEY: I am afraid I can't answer. I just don't know. I just don't know specifically. We are working in that field and I would say yes, that we have other agencies involved through the Joint Strike Force, because many of these things quite probably would be a violation of Internal Revenue regulations and rules and laws, and so most of these in the Joint Strike Force—there is another agency involved, maybe not at the beginning but at the end, certainly.

Gambling violations—cases have been turned over after a certain point to IRS to determine whether there was in fact any violation of IRS regulations.

MS. SHIENTAG: Would the old activity that was carried on by Lepke that Tom Dewey successfully terminated—it is continuing more or less in a modified form?

MR. SWEENEY: Well, I would say it is quite modified. I don't think that you are going to find the old labor shake-down, Capone. I have heard of recent instances where they are extorting protection money as they used to call it. There are certain instances of it but I don't think it is as prevalent as it was back in the Lepke days.

MR. SHIENTAG: Do you think the techniques that you have been allowed to use under the Title III have helped? Has it been one of the weapons that has limited extortion?

MR. SWEENEY: I would say you can't just limit it to extortion, but Title III has been perhaps one of the greatest weapons that law enforcement, the FBI, has had in the fight on organized crime. I guess there is really nothing to compare to it.

MS. SHIENTAG: Thank you very much.

MR. SWEENEY: Thank you.

CHAIRMAN ERICKSON: Professor Blakey.

PROFESSOR BLAKEY: Mr. Sweeney, I was very fascinated by the questions of Mr. Cook in reference to the area of theft and fencing. I look at the annual statistics for last year which is January 1 through December 31 of '74, and it indicated on the Federal level there were 68 gambling taps, 62 narcotics taps, but only 9 possession or receipt of stolen property.

MR. SWEENEY: Yes, sir.

PROFESSOR BLAKEY: And I wonder if you would share with the Commission why more profit cannot be gotten from electronic surveillance in this area.

It seems to me from what I know of the fencing operations, they are as potentially vulnerable to surveillance as gambling.

MR. SWEENEY: There are several reasons, one of which I outlined to Mr. Cook. One is the fact a given location may not be handling a stolen load

during the period in which it is in. In other words, we could go 15 or 20 days.

Second, we have had some fair success without the use of Title III in the breaking of hijacking cases.

PROFESSOR BLAKEY: I am not thinking of just hijacking, but more properly of fencing, which is the other half of it. Nobody hijacks a truck unless he's got a place to sell it.

MR. SWEENEY: It is part and parcel of the same crime, really. And I daresay that we certainly arrest more fences than we do hijackers, inasmuch as the hijacker has possession of it for a brief period of time. He then turns it over to the fence who has the task of getting rid of it all at one time or piecemeal-ing it out. So he is usually more vulnerable than the hijacker.

The fence, if he is found with the stolen goods, is immediately arrested on the spot and we have an excellent case against him.

PROFESSOR BLAKEY: What I am wondering, though, is why you are thinking just about knocking off fences for the possession and sale of stolen property. Wouldn't it be better to find out if he is a fence, put him under electronic surveillance and cover him for a while, since he must be dealing with thieves on a regular basis, and then if he is a fence, go in and arrest him and pick up half the thieves in town, too?

The difference between that and a gambling case is if you go in on a gambling case the customers are not committing crimes, so their incriminating conversations are not incriminating as to them, but only as to the gambler. If you stayed in on a thief, wouldn't you pick up all the thieves?

MR. SWEENEY: The probable cause, as we outlined, would be difficult. We enter into any theft of property, stocks, bonds, cargo, what have you, under two major laws, the theft from interstate shipment law, and interstate transportation of stolen property.

PROFESSOR BLAKEY: Supposing you had a theft statute like 1955, which required you to show merely an impact on commerce rather than individual interstate trips. Would that facilitate your ability to do it?

MR. SWEENEY: It would have to, yes. In other words, you are removing the interstate aspect of it.

PROFESSOR BLAKEY: Or substituting for the interstate aspect an "effect on commerce."

MR. SWEENEY: Most of our information which would support an affidavit for Title III would come from either of two means. One would be live informants and the other observations. These are the two principal sources of our affidavit. It is very difficult from an informant or from observations to

say that at a given location cargo stolen in interstate shipment is being fenced.

PROFESSOR BLAKEY: So the reason you are not doing more has nothing to do with Title III. It has something to do with 659.

MR. SWEENEY: It is probable cause in 659. That is one of the reasons.

PROFESSOR BLAKEY: Let me ask you again. Do you have a problem once you put in—and I see you have last year—fencing-type taps or bugs? How long can you afford to leave one in to pick up thieves? Is there any problem in that?

MR. SWEENEY: You mean from a technical standpoint?

PROFESSOR BLAKEY: Technically you can leave them in for as long as you have probable cause?

MR. SWEENEY: Yes.

PROFESSOR BLAKEY: But I am talking about a practical standpoint.

MR. SWEENEY: The monitoring or the manpower situation?

PROFESSOR BLAKEY: Maybe I should ask the question in a more straightforward fashion. I have had it put to me before that you can stay in on a gambling tap long enough to pick up the next level and you can jump. You can stay in long enough on a narcotics tap until you pick up the next level and jump.

Can you stay in that long on fencing taps or do you have a problem with learning that a hijacking is going to occur?

MR. SWEENEY: Well, yes, that would be that the tap would come down at the time we learned the hijacking was to occur. Then we also have the problem in an armed hijacking—it is armed. There is a gun involved and there is a life in danger. So we have to make some overt act. We can't just stand by and let this happen.

An armed hijacking is one of the—pre-knowledge of an armed hijacking is an extremely difficult situation because you know, say, at a given time that somebody is going to put a gun to somebody else's head. And it is a delicate situation as far as handling is concerned, probably one of the most delicate.

PROFESSOR BLAKEY: So that would limit your ability to stay in on a fencing tap?

MR. SWEENEY: Oh, yes.

PROFESSOR BLAKEY: Is that the kind of information you could expect to get in one?

MR. SWEENEY: I would think that in coverage of something like this, we would hear the planning of certain hijackings. We would hear conspiracies involving hijackings, and we would certainly hear the fencing activities involving hijackings.

PROFESSOR BLAKEY: Do you have any problems with the bureaucratic organization of the Bureau? What I am thinking now is that typically Division 9 handles gambling and LCN, whereas Division 6 handles interstate theft. How much flow back and forth is there between those two divisions?

MR. SWEENEY: Well, of course, I can best speak for the field, the New York office. We have a constant flow between our Hijacking Squad and our Division. It is a daily thing.

PROFESSOR BLAKEY: Do you know whether this is common throughout the Bureau?

MR. SWEENEY: I assume that it is but nobody, I would say, in the hijacking field has the—I mean nobody in the FBI has the hijacking problem that New York has. I think when you discuss truck hijacking you are basically discussing New York City.

PROFESSOR BLAKEY: That is not true of fencing?

MR. SWEENEY: No.

PROFESSOR BLAKEY: Are the Division 6 people integrated into the Strike Forces, or the Strike Force liaison people, like Division 9?

MR. STAFFELD: Insofar as the Bureau's representation on the Strike Force is concerned, it is a Bureau matter, not Division 9 or Division 6.

PROFESSOR BLAKEY: It ought to be that but you know there are separations.

MR. STAFFELD: It is still a Bureau representative and not a Division 9 representative as opposed to the Division 6 representative.

PROFESSOR BLAKEY: Is the guy with the Strike Force from Division 9?

MR. STAFFELD: In New York?

PROFESSOR BLAKEY: Throughout the country.

MR. STAFFELD: The man who is working with the Strike Force in the Southern District is representing the New York office. He is not representing a particular division.

PROFESSOR BLAKEY: Does he have any bureaucratic status within the Bureau? Is he in 9, 6, or a supervisor?

MR. STAFFELD: He is an agent of the New York office and we do not lay claim at the seat of government to any particular agent in the field.

PROFESSOR BLAKEY: They are assigned to a squad, though, aren't they?

MR. STAFFELD: There is an Organized Crime Squad in the New York office which does, by normal procedure, do business with our Organized Crime Section at the seat of government, that's true.

PROFESSOR BLAKEY: And they are the ones who do business with the Strike Force. And the Organized Crime Squad does handle fencing cases typically.

MR. STAFFELD: That is true, but on the other hand, there may well be a theft of government property or there may be an interstate transportation of stolen property case which involves an organized crime figure. And this will be handled by what we call Division 6.

PROFESSOR BLAKEY: In the Strike Force?

MR. STAFFELD: At the seat of government. It will be handled by the Strike Force in New York and by Division 6 at the seat of government and Division 6 may be in touch with Bill Lynch in the Organized Crime Section in the Department of Justice.

PROFESSOR BLAKEY: I have no further questions.

CHAIRMAN ERICKSON: Mr. Westin.

MR. WESTIN: I have no questions.

CHAIRMAN ERICKSON: I just have a couple, Mr. Sweeney.

You have stated that organized crime is today big business. In the period that you have been with the Federal Bureau of Investigation, has the operation become more sophisticated or less sophisticated?

MR. SWEENEY: Organized crime?

CHAIRMAN ERICKSON: Yes.

MR. SWEENEY: I would say it has become more sophisticated. Certainly as law enforcement becomes more sophisticated they have more safeguards they have drawn up to protect themselves. And it varies from area to area but they are quite sophisticated, no doubt about it.

CHAIRMAN ERICKSON: And their operation goes into various businesses, all types of operations?

MR. SWEENEY: Anything in which they can make a profit.

CHAIRMAN ERICKSON: As a result, the investigative tools that you had to fight organized crime in 1930 are not the same as they are today?

MR. SWEENEY: That is true, sir.

CHAIRMAN ERICKSON: And the tools that you had for the old type of organized crime wouldn't dent the surface of the present operation?

MR. SWEENEY: Not at all; not at all.

CHAIRMAN ERICKSON: So the techniques that you have to use have to meet the computer age?

MR. SWEENEY: That is correct, sir.

CHAIRMAN ERICKSON: And electronic surveillance is essential to your operation?

MR. SWEENEY: It certainly is. It is one of our greatest weapons.

CHAIRMAN ERICKSON: That is all.

Mr. Sweeney, we are indebted to you.

It is 12:22 at this point. We will recess. There is no reason to commence the next witness. The Commission, itself, has some internal business that will be taken up at this point.

We will be reconvening at 1:45 in Room 1318 in the Dirksen Building. They weren't able to afford us this facility this afternoon.

Gentlemen, I thank you for being with us and we will see you this afternoon.

[Whereupon, at 12:25 p.m., a luncheon recess was taken until 1:45 p.m.]

AFTERNOON SESSION

PROFESSOR REMINGTON: I think we are ready to reconvene.

I see a very distinguished group before us this afternoon. I am starting this session because our chairman, Judge Erickson, may be a very few minutes late and he asked me if I would start, and we are going to turn next to Mr. John Barron.

I understand, Mr. Barron, that you have already been sworn.

MR. BARRON: Yes.

TESTIMONY OF JOHN BARRON, SUPERVISOR, ORGANIZED CRIME DIVISION, FBI, LOS ANGELES; ACCOMPANIED BY ALVIN A. STAFFELD, INSPECTOR, AND JOHN E. KELLY, JR., INSPECTOR, FEDERAL BUREAU OF INVESTIGATION

PROFESSOR REMINGTON: Perhaps as a start, Mr. Barron, you could tell us about your general law background and experience and after that I will turn it over to Dave Cook, who fortunately has arrived in the nick of time.

MR. BARRON: I have been a Special Agent for the FBI for 21 years and since 1961 have been assigned to work or supervised work on organized crime in the Los Angeles office.

All of my experience concerning organized crime is, in fact, in the Los Angeles area.

For a year I was assigned back to Headquarters in the Organized Crime Section, from 1969 to 1970.

Prior to 1961, I worked on various types of work, including jewel thefts, internal security, in the Miami office.

PROFESSOR REMINGTON: David.

MR. COOK: Thank you, Mr. Chairman.

Mr. Barron, you are heading the squad which at this time has jurisdiction over illegal gambling operations in Los Angeles?

MR. BARRON: That is one of the two squads that I am coordinating supervisor of.

MR. COOK: Do you have fairly close liaison with that squad? Are you in contact with its daily operations?

MR. BARRON: Yes, I am.

MR. COOK: Do you know approximately how many Title III surveillances you have directed at gambling in Los Angeles, say in the last six years, or during your experience?

MR. BARRON: Approximately 24.

MR. COOK: Have all of these been under Section 1955 or have you had some interstate operations as well?

MR. BARRON: We have had interstate cases under laws passed in 1961.

MR. COOK: To the extent that those cases are closed—I'm sure you recall from our study in Los Angeles, we are dealing only with closed cases—what was the structure of the interstate violations in those cases where you had interstate gambling surveillance?

MR. BARRON: It would concern itself principally with lay-off activity between the states of California, Nevada, New York, and some of the southern states.

There would be gamblers in Los Angeles who had been using the telephone facilities to relay bets and instructions concerning betting or activity concerning betting to other states or receive it from other states, concerning line information as well as instructions on betting.

MR. COOK: Have you been active in interstate types of interception since the enactment of the Illegal Gambling Business statute?

MR. BARRON: Yes, we have.

MR. COOK: And did you find the requirements for jurisdiction in Title 18 Section 1952 or in 1084?

MR. BARRON: Yes.

MR. COOK: Did you find the requirements for jurisdiction in those are easier met than the requirement of 1955?

MR. BARRON: I would say they are the same. You are talking Title III? You are addressing yourself to Title III?

MR. COOK: Right.

MR. BARRON: I would say it is no more difficult to write an affidavit or investigate a case, so to speak, where an affidavit would be used, dealing with those involved in the violations of 1955 than those in 1084.

It would be the same information, informant information, surveillances, the same activity.

MR. COOK: Can you compare your success in prosecutions? Is there any difference in your success in prosecuting Section 1955 as opposed to 1084?

MR. BARRON: Are you talking now about the sentencing?

MR. COOK: Let's first relate it to the convictions because I understand sentencing is another area.

MR. BARRON: While some of the cases in which we used the Title III technique are pending grand jury action or pending trial, and while others are not completed by virtue of being in an appeal status, none of the affidavits and the resulting Title III's have failed to produce the evidence we anticipated when we sought to use this technique.

MR. COOK: This is in each of your surveillances?

MR. BARRON: Yes.

MR. COOK: What is the situation with regard to the sentencing in those cases in which you obtained convictions for gambling violations?

MR. BARRON: That varies, of course, with the judge, and the individual judges will sentence in accordance with their own thoughts or whatever structures their sentencing procedures.

With some judges we get stiffer sentences than we do with others.

MR. COOK: Can you make any general characterization? Are you satisfied with the type of sentences you are getting? Do you think it is sufficient for enforcement purposes?

MR. BARRON: My own personal feeling is I am not satisfied, no, because I know the people I am dealing with are involved in organized crime activities and I would like to see a stronger sentence, yes.

MR. COOK: Perhaps we could put that in the context of whether or not the sentences you have been obtaining have had a deterrent effect on the bookmakers in Los Angeles.

MR. BARRON: Sentencing results in the break-up of his operation and assessments by Internal Revenue. He may go back and be structured differently. He certainly in many instances is smaller in operation size. So it is a deterrent.

Should this not have occurred, should there have been no trial or arrest, his operation would only have grown. So I would say that it is a deterrent.

MR. COOK: You do have an organized crime family, so to speak, in Los Angeles, do you not?

MR. BARRON: Yes, we do.

MR. COOK: I think you indicated at the time of our interview that this was run by Dominic Brooklier?

MR. BARRON: Yes.

MR. COOK: To what extent is the syndicated family involved in gambling in Los Angeles?

MR. BARRON: To the extent that they shake them down. In other words, a bookmaker pays protection money to them.

MR. COOK: Are the family members not ordinarily active as bookmakers?

MR. BARRON: No; they don't sit on the phone.

MR. COOK: Do they act as bankers?

MR. BARRON: They risk nothing. They only take profits. In other words, they say "Meet your new partner and I don't want to hear about your losses."

MR. COOK: And what are the consequences if they don't receive that kind of cooperation?

MR. BARRON: They threaten them.

MR. COOK: Have you had any instances of extortion investigations or prosecutions resulting from this type of shake-down operation you have just described?

MR. BARRON: Yes.

MR. COOK: And how successful have these been?

MR. BARRON: Very successful. We prosecuted the head of the family and his under-boss just last month.

MR. COOK: And has that case come to a conclusion?

MR. BARRON: Final sentencing is June 16.

MR. COOK: And can you tell the Commission who was convicted as a result of that operation?

MR. BARRON: The boss, Dominic Brooklier; his under-boss, Sam Sciorentino, Peter John Milano and seven others that were operatives for them.

MR. COOK: And I think you indicated that Peter Milano was related to a member of an organized crime family in Cleveland?

MR. BARRON: A son.

MR. COOK: Is that right?

MR. BARRON: He is a son of a member in Cleveland.

MR. COOK: So this would tend to confirm the existence of the national nature of LCN, to use the term.

MR. BARRON: Yes.

MR. COOK: How many agents do you have on your Gambling Squad?

MR. BARRON: I might address myself to both squads because we work together.

MR. COOK: All right.

MR. BARRON: It is divided by what we call classifications merely to have certain manpower on each of the two squads, but they are interchangeable. So the answer to that is 46.

MR. COOK: Forty-six?

MR. BARRON: Yes.

MR. COOK: And what is your total office complement in Los Angeles?

MR. BARRON: Five hundred.

MR. COOK: What capability or what method do you use for development of intelligence in Los Angeles?

MR. BARRON: First of all, there is police liaison, the exchange of information with other law enforcement agencies, directly or through the

Strike Force. Of course, the basic and best is the informant. The ability to target individuals who are in a position to furnish information on a long-time basis, right to the heart of organized crime as close as you can get and give it to you on a continuing basis and it is quality information—that is the basic structure of your intelligence. And with that—everything else keys on it. In other words, as you learn certain information you take certain action, surveillances, interviews, maybe grand jury subpoenas, maybe the grand jury method, immunity grants, or the various methods open to us—or a Title III. But it is your information that comes from your informant program that rounds out your intelligence.

MR. COOK: Do you have a specific agent or group of agents assigned to development of an informant program?

MR. BARRON: I have those that are assigned for the coordination of it. Each man assigned to the Organized Crime Squad is required to participate in the informant program.

MR. COOK: And am I correct in making the assumption that informant information is the basis for most, if not all, of your Title III surveillances?

MR. BARRON: I know of no exception as to the very early basic source of the cases.

MR. COOK: It has been suggested that the FBI, in maintenance of its informants, sometimes protects people who continue to violate the law for the purpose of obtaining intelligence. I am not intimating that that is the Commission's view, but it is one of the criticisms that has been made of the Bureau operations.

Can you explain to the Commission—and this is based on an interview in Los Angeles—your philosophy as to the informant development and the use you make of informants at particular times and the need for concealing informant identity?

MR. BARRON: Informants are individuals—and we are speaking of organized crime activity—are individuals who are very reluctant to talk to us at the outset due to the code of the underworld. For many and varied reasons and sometimes for reasons unknown, an individual may elect to cooperate with law enforcement on a confidential basis. They present at the very outset this as the only condition under which they will talk. They will never testify, because they fear retaliatory action from their associates should they testify.

We, in turn, tell them that their cooperation with us does not condone any illegal activity on their part. And I know of instances where we have developed informants and they are in the stage of being developed and they weren't telling us candidly what was going on and we found out they

were involved in an ongoing conspiracy and we indicted them.

So we do not allow or permit, in the FBI, our informants to engage knowingly in illegal activities.

MR. COOK: I think you made the distinction in our discussion on informants and the necessity at times to reveal the identity or to make the decision to conceal them.

The distinction you made between hip-pocket or throw-away informants and the type of informant that you develop as I think what you call a top-echelon, TE, informant—

MR. BARRON: I think you may have asked about throw-away informants because we don't have any such thing.

MR. COOK: I didn't say you said that. I said you distinguished between that type of informant which may exist in the course of other agencies' work. But you did indicate that you felt it was sometimes necessary to maintain the continuation of an informant in order to develop strategic informants as well as the commission of specific criminal offenses.

MR. BARRON: Knowing what is going on today and what is going to go on tomorrow.

MR. COOK: And you do have to rely on informants for identification of their LCN membership.

MR. BARRON: As someone said here earlier, it is no crime to belong to this organization, the LCN. That is not a violation. So, while we like to know who is in it and who is not in it, the mere fact that they are in it is not really what we are after. We are after what they are up to that is illegal.

MR. COOK: Now, in terms of relating this to informants, do you make much use of consensual recording devices in Los Angeles?

MR. BARRON: Yes, we do.

MR. COOK: Do these include both body recorders as well as telephone recording?

MR. BARRON: Yes.

MR. COOK: What would be the effect on your operations if consensual recordings of either type, either the telephone type or body transmitter, were placed under the court-ordered system?

MR. BARRON: First of all, in organized crime it is usually an ongoing situation in which there is threat and it is a "now" situation. If we get a call there is going to be a meeting tonight and it is concerning a shake-down, naturally we couldn't go through the Attorney General or get a court order in that period of time.

Second, we must deal with other violations, such as kidnaping in which a son may be the kidnap victim, and the parent is diverted from phone to phone to phone for additional instructions. With consensual monitoring we are able to record and attack

the case. We certainly couldn't run to court each time he receives instructions to move to another phone. It would not be workable.

MR. COOK: Within the time situation that you described, the FBI does have a capability of emergency use of a consensual device with a follow-up written confirmation to Headquarters; isn't that right?

MR. BARRON: We get it from our Headquarters here in Washington.

MR. COOK: So in a case, for example, where you were involved in a kidnaping and going from phone to phone to phone, you would not have to go through the administrative procedure each time you wished to make a recording of the phone?

MR. BARRON: For consensual monitoring the authority is granted for the phone by the special agent in charge of the district. The body recorder—the authority for that has to come from Washington.

MR. COOK: I see.

How do you make the selection, if you do make the selection, of the case agent who will be in charge of the Title III investigations?

MR. BARRON: First of all, we do all this investigation prior to the Title III being applied for. While the case is being investigated it is assigned to an agent. That is the agent that walks it through the Title III course, whoever is assigned it. Any agent could have the capability of having a case that will result in a Title III.

MR. COOK: Does that mean the case agent who had the first major informant contact relevant to the violation?

MR. BARRON: No. My assignment of cases to agents by myself and other supervisors is based on the activities of the agent, who is involved in what. Some agents may have just finished a prosecution and their case is ended and so we have a case today that will go to him because what we call his workload allows it. And he then, in working that case, might just come up to a Title III. The selection is made by the supervisors, not by someone who writes up information from an informant and comes to me—if there is no case open on that at the time and it is new information, I would open it and select an agent based on his workload.

MR. COOK: I see. So you do function as an intelligence coordinator; is that true?

MR. BARRON: Yes.

MR. COOK: Do you take any special measures to train your agents in the conducting of a Title III investigation, or is this something that is learned more or less on the job or the basis of contact with other more experienced agents?

MR. BARRON: Well, we do have training in all facets. It is an ongoing thing. There is training for surveillances, training for writing affidavits—not necessarily Title III affidavits—affidavits of search, affidavits of other kinds that are used. And agents are trained constantly in report writing; they are trained in administrative procedures; they are trained in identifications—all types. And in that they are trained, and the training is constantly going on—there are courses of instruction that involve Title III's, yes.

MR. COOK: How closely is the work of the case agent associated with the work of the supervisory attorney?

MR. BARRON: At the time of the Title III?

MR. COOK: Yes.

MR. BARRON: Extremely close—daily, hourly, sitting with him going over it.

MR. COOK: Do you also have a responsibility for being in contact with the supervisory attorney or do you have other duties which require you to be busy doing other things?

Do you have enough time to work with the supervisory attorney or is that necessary?

MR. BARRON: Oh yes, I do. You have to take time for that. Is anything suffering as a result of my giving time to that? No.

MR. COOK: No, I wasn't inquiring about that. I was just inquiring as a matter of fact.

MR. BARRON: Yes, we work on a caseload approach and that permits us to do what has importance.

MR. COOK: And you said you had Title III investigations on gambling?

MR. BARRON: Right.

MR. COOK: Do you know how many Title III investigations you have had in other areas in that time?

MR. BARRON: Two.

MR. COOK: What areas have those been in?

MR. BARRON: Labor racketeering and hoodlum shakedown activities.

MR. COOK: Are these cases closed?

MR. BARRON: No.

MR. COOK: They are ongoing?

MR. BARRON: Yes.

MR. COOK: Without revealing any of your investigative strategies, do you contemplate the use of the RICO statute in connection with electronic surveillance?

MR. BARRON: It has violations within it that lend itself to it, yes. Yes, RICO is one that can be used. Yes.

MR. COOK: You were active in organized crime enforcement prior to the availability of Title III; is that right?

MR. BARRON: Yes, I was.

MR. COOK: And what methods did you rely on at that time in attempting to enforce the federal laws?

MR. BARRON: Developing witnesses who would testify.

MR. COOK: And did you have much success in doing that?

MR. BARRON: In interstate gambling, none. Interstate travel law violations—for someone to travel from Point A to Point B, we developed through witnesses individuals who would testify to the gambling and the interstate travel. And we supported it.

I think another case in point would be the Zerilli case out of Detroit where Zerilli and Giordano came in and had meetings in Nevada. We have had good success other than Title III's.

MR. COOK: As a result of the convictions of Brooklier and Sciorentino and other defendants in that case, have you been able to detect a change or disruption in the pattern of organized gambling in Los Angeles?

MR. BARRON: Sir, when the fellows were on trial they were still shaking people down. Now, when they go to jail they will stop, but there are people there that will continue. Or there are people from New York or Detroit that are going to come in.

MR. COOK: When you say "people from New York or Detroit," is Los Angeles from an organized crime standpoint vulnerable to intrusion by families from other cities?

MR. BARRON: Basically they can't come in and operate in the town. But they can operate businesses. They will tell them, and perhaps cut them in on it.

MR. COOK: I see. Without the existence of Section 1955, do you think you would be able to penetrate and prosecute these operations with any degree of success purely through the use of informants, without Title III?

MR. BARRON: No. You mean search?

MR. COOK: Well, I assume—

MR. BARRON: Or do you mean informants testifying?

MR. COOK: Either way—informants as witnesses—

MR. BARRON: I wouldn't get any to testify. And searches—yes, you could have prosecution for searches. We do. But you wouldn't get the whole operation. And if we didn't have 1955, we would still have tried to investigate and prosecute gambling. If we didn't have Title III we would still continue, but we wouldn't be as effective.

MR. COOK: In terms of enforcement of Section 1955, what kind of considerations do you make as far as evaluating the significance of the Illegal Gam-

bling Business which, even though it may meet the statutory requirements, is not what you might consider an organized crime statute?

MR. BARRON: We would send it to the Los Angeles Police Department or other appropriate agency.

MR. COOK: Has that proved effective?

MR. BARRON: Yes.

MR. COOK: Thank you, Mr. Chairman.

CHAIRMAN ERICKSON: Professor Remington.

PROFESSOR REMINGTON: Mr. Barron, I think it is a fair summary of the testimony we have heard with regard to gambling that there are a number of different views. One is I think the view you expressed that there is need for enforcement and Title III is very important to effect that enforcement.

MR. BARRON: Yes.

PROFESSOR REMINGTON: Some people have appeared before this Commission and said that gambling is really not sufficiently important to waste time and effort on and they have said they turn their efforts in different directions, and I think some have even gone to the point of saying that the cure for the gambling business is probably legalized gambling.

What I am really searching for is, in this Commission's responsibility to determine how important Title III is, what we ought to say with regard to gambling. Because if one says, as you have said, that Title III is important to enforcement of gambling cases, the response anticipated from some, including some members of the law enforcement profession, is "So what? It's not that important. So you shouldn't have wiretapping for that purpose."

MR. BARRON: I don't share that view.

PROFESSOR REMINGTON: That was just to lay a basis for asking you really what you think the Commission ought to say in response to that. What is the answer to the assertion that you don't need wiretapping in gambling cases?

MR. BARRON: Sir, I think you have to address yourself to the fact that gambling and extortion to our knowledge have been the backbone and mainstay of organized criminal activities. To say that attacking it isn't hurting them, I think would be faulty.

If a man only has \$10 and you take away five of it, you have hurt him. If you allow them with impunity and immunity just to run around and increase it, then of course you are not attacking it any longer—if that answers the question.

PROFESSOR REMINGTON: So I take it you say Title III is important in dealing with gambling cases and dealing with gambling cases is important in dealing with the problems of organized crime?

MR. BARRON: Yes, sir.

MR. STAFFELD: I think, sir, it goes even further than this, because when this individual gets to the point where he owes the gambler money and he has to make good on this debt, we find that many times he ends up in other endeavors of crime; he is in pocketbook snatching or bank robbery or breaking and entering. So this business of organized gambling and the organized crime people having their hooks in people contributes to an awful lot of other crime. That is the reason we think we have to have Title III to cut short organized gambling which, in effect, we think has another end product insofar as the over-all crime picture is concerned.

PROFESSOR REMINGTON: Would this continue to be true if those who urged decriminalization would be successful throughout the country? If we could anticipate the possibility of a day when in most states gambling would be legal, would the problem still exist?

Again, I want to indicate one of the problems I have. One says electronic surveillance is effective to deal with gambling and gambling has these serious consequences. And one answer to that is, "Yes, because we make gambling criminal when it shouldn't be. It is consensual activity and the way to do it is not to have electronic surveillance, but to legalize gambling."

Is that a good answer?

MR. KELLY: I am not addressing your question directly but there is one crime that relates to gambling in a cause-and-effect relationship—loansharking, probably one of the most vicious crimes the FBI investigates.

Loansharking would probably be about the third most lucrative source of revenue for organized crime in the United States, gambling being number one, and then narcotics and loansharking. You are going to have loansharking offenses even if you legalize gambling. You are not going to get away from that. And we have had example after example of people that get caught up in this in a big debt, borrow, lose everything, and it is a proven fact that in many of these cases the violence attendant to loansharking is organized crime at its worst.

PROFESSOR REMINGTON: In your judgment, if gambling is legalized more broadly across the country, would loansharking increase or decrease or remain the same?

MR. BARRON: I think it would remain constant. Without specifically citing an ongoing case, let me make brief reference to an individual in private enterprise who lost extensively at the legal gambling tables in Las Vegas. His senior position in a major corporation made him vulnerable and as a consequence, he was prevailed upon to perform a service which was not only unethical but illegal as

well. While this was not a true loansharking situation, it certainly was an extortionate conduct arising out of a gambling debt.

PROFESSOR REMINGTON: Let me just ask one final question. Is that more likely to happen in gambling than it is if this man had business reversals or something else?

MR. BARRON: The shylocks don't hit only the gamblers. They are willing to provide their services to anybody and it often includes persons who cannot otherwise establish a legitimate loan or source of credit.

PROFESSOR REMINGTON: But I take it gambling is a major contributor toward loansharking and would be even if it were legal.

MR. BARRON: Another thing I argued is you could set up in every corner store a place to bet legally but the advantage to gamblers is the credit and the telephone. In other words, the people that bet are in their office of a stock brokerage firm or the banker or the doctor who just picks up his phone and calls his bet in. If he has to get in his car and go down and bet legally with the state, he won't—but you will not stop your illegal bookmaking.

MR. KELLY: I would like to add one note on legalized gambling—I am not taking a position on it but we have run surveys of those states that have lotteries, OTB, in New York, for example, and we couldn't find where this had any impact on the illegal gambling. This business was still flourishing. We may be developing a new group of bettors, people that wouldn't bet illegally because it is against their nature. But you are not stamping out illegal gambling by legalizing, let's say, state lotteries.

PROFESSOR REMINGTON: Thank you.

CHAIRMAN ERICKSON: Chief Andersen.

CHIEF ANDERSEN: I have a couple of questions. One area we haven't gone into is the FBI and their equipment. Do you maintain your own tapping equipment in Los Angeles, your own inventories?

MR. BARRON: Yes.

CHIEF ANDERSEN: Do you maintain your own inventory control there or in the Washington office?

MR. BARRON: In both places.

CHIEF ANDERSEN: You have a dual system of keeping track of it? A double check?

MR. BARRON: Yes.

CHIEF ANDERSEN: This way you always know where your equipment is. There is no chance of it being misplaced?

MR. BARRON: That is right, no chance.

CHIEF ANDERSEN: What telephone company serves Los Angeles?

MR. BARRON: Two, AT&T and General Telephone—Pacific Telephone and General Telephone.

CHIEF ANDERSEN: How is your cooperation with them?

MR. BARRON: Good.

CHIEF ANDERSEN: No problem with lease lines?

MR. BARRON: When we have a court order.

CHIEF ANDERSEN: They follow the Federal mandate?

MR. BARRON: When their attorney receives the court order and not until then.

CHIEF ANDERSEN: But you do not have disputes over the probable cause in the court order?

MR. BARRON: No, not if the court signs.

CHIEF ANDERSEN: The reason I ask is that we have heard of problems in other jurisdictions.

MR. BARRON: That is not true in Los Angeles. They accept the court orders.

CHIEF ANDERSEN: It is my understanding that Federal Title III information is not admissible in a California State court.

MR. BARRON: That is correct.

CHIEF ANDERSEN: What problems does that create for you?

MR. BARRON: None. It hasn't yet.

CHIEF ANDERSEN: What problems does it create in the exchange of information between the local police and you?

MR. BARRON: They can't use my information.

CHIEF ANDERSEN: Do they have access to it?

MR. BARRON: No.

CHIEF ANDERSEN: No access, at all?

MR. BARRON: No.

CHIEF ANDERSEN: Would it help both your agency and the State authorities, if they could use your intelligence?

MR. BARRON: I am sure it would help them if they could use state wiretap law or use ours.

CHIEF ANDERSEN: I mean just use the information.

MR. BARRON: Sure.

CHIEF ANDERSEN: Would it help if it could be done legislatively through Title III?

MR. BARRON: Yes.

CHIEF ANDERSON: Do you think it is worth pursuing by this Commission?

MR. BARRON: There could be a circumstance in which we would hear something of a homicide nature.

CHIEF ANDERSEN: What would you do if you were listening on a wire and somebody said they were going to kill—

MR. BARRON: We would tell them. The Strike Force would tell them. We would go to the attorney and judge with it, but we would tell somebody.

CHIEF ANDERSEN: That is all I have, Mr. Chairman.

CHAIRMAN ERICKSON: Thank you very much, Chief.

Judge Pierce.

MR. PIERCE: I believe you testified that agents receive training with respect to Title III; is that correct?

MR. BARRON: That is right, sir.

MR. PIERCE: Precisely what kind of training do they receive?

MR. BARRON: How to frame and affidavit, how to write probable cause. I could liken it to how to write a report in one of our violations. It is a normal training procedure.

MR. PIERCE: Are they trained as to what situations warrant a wiretap?

MR. BARRON: Yes, where the law applies, in other words, to actually read the bill.

MR. PIERCE: Do they get trained as to what circumstances would justify a wiretap?

MR. BARRON: Not specifically, no, because that is a decision that is made more or less by myself and that agent at the time. He comes to me at the end of his investigation. I have a surveillance squad that is at his disposal. We have checked it out. They corroborate what we have learned from informants. We have watched the man's activity to see who he meets with. He is meeting with people that the informant claims he is meeting with.

MR. PIERCE: In other words, they learn what situations warrant a wiretap on the job, so to speak?

MR. BARRON: Yes, sir, as it is developed. He will come in and say what shall we do, and we say let's check with a couple more informants.

MR. PIERCE: In other words, there is no formalized course on how to do it?

MR. BARRON: No, I don't know how I would give one. I don't know what I'd tell them as concerns that.

MR. PIERCE: I have nothing further.

CHAIRMAN ERICKSON: Thank you very much, Judge.

Judge Shientag?

MS. SHIENTAG: No questions.

CHAIRMAN ERICKSON: Professor Blakey.

PROFESSOR BLAKEY: Mr. Barron, you indicated earlier that during a number of organized crime type investigations you had situations come up—and you illustrated kidnaping—where you couldn't get a court order in the consensual area.

MR. BARRON: Yes, sir.

PROFESSOR BLAKEY: Have you had occasions in organized crime type investigations where a meeting would occur say in a hotel or a motel, where you would know about the meeting an hour or an hour and a half beforehand, say over a wire, where, if you could get to the hotel in time you could have gotten coverage of the meeting—

MR. BARRON: You mean a Title III?

PROFESSOR BLAKEY: Well, given a Title III, technically you could have gotten to the hotel and put a device in the room or on the wall next to the room.

MR. BARRON: You mean physically it is possible, yes.

PROFESSOR BLAKEY: Is that common experience in your investigation?

MR. BARRON: No.

We are addressing ourselves now to a body recorder type situation.

PROFESSOR BLAKEY: Well—

MR. BARRON: You are talking about two people, neither of whom would be cooperative with me and we have informant information that they are going to meet today at a hotel or motel or restaurant to discuss some criminal endeavor. Do I learn of that? Occasionally we do.

PROFESSOR BLAKEY: Where you learn that somebody is reporting back to somebody at a higher level and they get in a car and drive around?

MR. BARRON: Yes, that happens.

PROFESSOR BLAKEY: Frequently?

MR. BARRON: Well, it isn't as frequent as I would like to have that information because we would like to have it if we have the type of informants that tell us, but it happens.

PROFESSOR BLAKEY: Do I understand your testimony correctly to be if you were authorized to use the emergency provisions of Title III, and then get your court order within 48 hours, you could use it?

MR. BARRON: To establish probable cause for that—I would really have to satisfy a lot of people that what is going to go on down there would be of major importance.

PROFESSOR BLAKEY: If you had a wire—

MR. BARRON: I have a wire in one location and I am going to meet in another location.

PROFESSOR BLAKEY: That is right. He said "I am going to make a phone call from another phone booth." You know when it is going to happen.

MR. BARRON: If I have heard it on the wire that he is going to call Joe at four o'clock on the phone and tell Joe, and I watch him go to the phone, I think I could use that.

PROFESSOR BLAKEY: That is true, but you can't use what Joe said on the phone?

MR. BARRON: No, I said I could use that information without a Title III.

PROFESSOR BLAKEY: I agree, but the only way you could get what Joe himself said on the phone—

MR. BARRON: —would be to monitor it, yes.

PROFESSOR BLAKEY: Or if two people—

MR. BARRON: I know what you are getting at. And I think—it would be nice. It would be a panacea of greatness. But from the standpoint of the dangers of that type of operation—

PROFESSOR BLAKEY: Let's explore the dangers of that kind of operation. One danger in a wiretap, I take it, is overhearing too much, that is, spillage. If you put a wire in for 15 days and you want two people's conversations with reference to gambling, very often you get the wife, and you have to minimize her out; you get the babysitter, and you have to minimize her out. But in the kind of emergency surveillance I am giving you, by definition, you only have two people meeting in a hotel room for a very short period of time. Aren't the dangers in that kind of quick overhear in a hotel room less than a ten-day wiretap?

MR. STAFFELD: No.

PROFESSOR BLAKEY: Why not?

MR. STAFFELD: In the first place, you are acquiring your probable cause over another source, another Title III. I think this is exactly where we are afraid somebody will make a misstep and completely take this technique away from us.

If the agent in Los Angeles says "Well, boy, I got this off this Title III. There is going to be a call made from X Hotel room and I, myself, am going to make the decision to cover that wire with no more than my own authority"—that we don't want.

PROFESSOR BLAKEY: I am not raising the question of possibility of abuse. What I am raising is there is an investigative need for it? If you don't have time to get a warrant in a normal search situation, you can bust in to save somebody's life. It seems to me that principle is applicable to electronic surveillance, too, and except for the one issue you raised, where some hotshot agent might jump where he shouldn't, why couldn't you institute internally within the Bureau the same kind of emergency provisions you have for consensuals and apply them to Title III's?

MR. STAFFELD: The very provisions of the Title III law, the emergency provisions, have never been extended to the Bureau.

PROFESSOR BLAKEY: That is my point, Mr. Staffeld. It seems to me there is a need for it, and if the technique is constitutional, and if you people can show responsibility, as you apparently have in the operation of Title III, maybe one recommenda-

tion of this Commission can be that the Attorney General implement that section.

MR. STAFFELD: Well—

PROFESSOR BLAKEY: You don't have to say—

MR. STAFFELD: Your point is well taken, but we aren't going to ask the Attorney General for that privilege.

PROFESSOR BLAKEY: What I really wanted to get at was the factual question. Do you have occasions in the course of your investigations where, all other things being equal, you could use it and use it with effect?

MR. BARRON: Yes.

PROFESSOR BLAKEY: I am very interested and wonder if you would kind of compare and contrast the organized crime picture you have in California. I am told that the situation is really different on the West Coast. For example, you have five families in New York, but you have one in Los Angeles. The five families in New York have gambling, narcotics, loansharking largely locked up, although they have problems with new groups now.

Is that the situation in San Francisco?

MR. BARRON: San Francisco?

PROFESSOR BLAKEY: Excuse; I'm sorry—Los Angeles.

MR. BARRON: No, we don't have five families, we have one—have always had one.

PROFESSOR BLAKEY: Approximately how large is it?

MR. BARRON: Membership? Thirty—thirty people.

PROFESSOR BLAKEY: It doesn't have organized crime locked up in the city?

MR. BARRON: No, it doesn't have Los Angeles locked up. It has organized crime—we view organized crime as being more than just the Mafia.

PROFESSOR BLAKEY: Well, if you can in just general terms, would you describe the Mafia and non-Mafia?

MR. BARRON: First of all, in Los Angeles we are finding, and I think more and more throughout the country—they will move in as testimony was produced earlier, into any avenue where income can be derived. There are families in New York that have controlling things in Los Angeles; in other words, pornography, so to speak, films, X-rated films, and magazines and books that are pornographic. We have more and more people going into what we call confidence schemes, stock thefts, embezzlements—

PROFESSOR BLAKEY: Both LCN people and other organized crime?

MR. BARRON: Or people working for it. It is hard for me to distinguish between a man who performs an illegal act and gives half to the LCN and

he is not one. They can grow by their numbers very rapidly, if you want to include the people who work for them, call them operatives, if you will.

PROFESSOR BLAKEY: Based on your general intelligence estimates, would you say the situation in California is less sophisticated, less hard-nosed, than in the East?

MR. BARRON: I have read about New York and know about it and I would say it is more vicious in New York.

PROFESSOR BLAKEY: People in California are not really different from people in the East, are they?

MR. BARRON: I know in Los Angeles inroads into that area would be most difficult because of the Los Angeles Police Department and their honesty—and other local law enforcement agencies, too.

PROFESSOR BLAKEY: Do I understand your testimony to be that the difference is found in a number of factors, and that integrity of law enforcement is a major one?

MR. BARRON: Yes.

PROFESSOR BLAKEY: Let me ask you then, since you raise it, about the Los Angeles Police Department. You have a liaison with them, I take it?

MR. BARRON: Very strong.

PROFESSOR BLAKEY: You work closely with them?

MR. BARRON: Very closely.

PROFESSOR BLAKEY: Am I right in assuming their reputation for not only integrity, but competency, is very high?

MR. BARRON: I can't compare, but I think in all law enforcement circles they are rated very high. They are very competent.

PROFESSOR BLAKEY: Now, you are operating in Los Angeles in a top-flight organization and you are watching a local top-flight organization. You've got surveillance and they haven't got it. Does that hurt their operations?

MR. BARRON: No, because I get a call from the Lieutenant and he says, "Hey, we are on Joe today," and I say—

PROFESSOR BLAKEY: No, I am saying if they had a state Title III.

MR. BARRON: Oh, Title III.

PROFESSOR BLAKEY: Would they be worth more?

MR. BARRON: Certainly.

PROFESSOR BLAKEY: In your judgment, are they inhibited because they don't have it?

MR. BARRON: Yes, in a bookmaking operation certainly, if they don't have a Title III.

PROFESSOR BLAKEY: Do you make better cases than they do laterally and vertically?

MR. BARRON: In gambling?

PROFESSOR BLAKEY: Gambling, extortion.

MR. BARRON: They make excellent cases in burglaries, robberies, extortion cases locally. They don't need a Title III for that and neither do we in most instances because there are 500 agents and I have only 46 of them and we are making a lot of cases in Los Angeles in other areas—thefts, stocks, other areas. And the Los Angeles Police Department gets their share of good cases.

PROFESSOR BLAKEY: I don't want to put you in the position of criticizing the LAPD. I am trying to contrast organizations operating in the same environment, one with surveillance, and one without, and trying to find out if it makes a difference.

MR. BARRON: Let me back up on that. The Los Angeles Police Department receives the same information that I do from an informant that a man is working at this number in an apartment house, and he is working for Joe Smith. The Los Angeles Police Department can take down that man on that line, right, by certain investigative steps, search warrant. And they will pick at a bookmaker and pick him to death because he has to rent new apartments, hire new people. It costs him. Compared to the Title III, we have the ability to get to what we call his back office room whereas, these front people, even if they wanted to testify, they couldn't. They couldn't identify him because they don't know him. They don't have his phone number. He phones them. So we are able to bring in the whole conspiracy and take it down. If they could have what I have they could do what I do.

PROFESSOR BLAKEY: Let me ask you this, talking about checking out of Washington consensuals or you running applications through—I know people in California, and when you try to talk to somebody in California from upstate New York, there is about an hour and a half a day you can get phone calls through.

MR. BARRON: I can make it in a minute anytime I want to.

PROFESSOR BLAKEY: If they work different hours.

MR. BARRON: I get them at home. I go right through the board and get them at home. I have never ever had a delay, because I know all of them here and if I didn't get one I'd get the other.

PROFESSOR BLAKEY: So, in fact, the time differentiation doesn't present a liaison problem?

MR. BARRON: We are talking about the five-minute phone call.

PROFESSOR BLAKEY: It doesn't to you but it does to them.

[Laughter.]

MR. BARRON: Maybe they don't like to be gotten out of bed but I still get them out of bed.

PROFESSOR BLAKEY: I was only asking whether it makes sense to decentralize some of the control over this.

MR. BARRON: I don't mind that control. That is just a phone call.

PROFESSOR BLAKEY: Let me ask you a concluding question.

You heard the conversation Mr. Staffeld and I had this morning?

MR. BARRON: Maybe I did. I don't know.

PROFESSOR BLAKEY: This is in reference to the "So what?" question. You have been in the Bureau for a number of years. You were in before the Organized Crime Control Act; you were in before Title III. You have now got immunity, you've got Title III, you've got adequate manpower—people who are honest and competent. In a sense, you've got about all we can give you except some embroiling of the details—"we" being society.

Have you really made a difference on the "organized crime problem"?

MR. BARRON: Yes. Yes. I would like to answer the question very affirmatively.

PROFESSOR BLAKEY: Please explain to me why you say yes.

MR. BARRON: Because we have put their leaders in jail. Every time they go to jail, that is one less that is in the street. If there are 30 of them and 5 are in jail, there are only 25 on the street.

PROFESSOR BLAKEY: Are any of them getting out of business?

MR. BARRON: Anytime they are in jail, they are out of business.

PROFESSOR BLAKEY: It is true a guy who is in the can is not on the street, and at a bare minimum that is a benefit. But isn't he being replaced by somebody else when he goes in the can? Don't you have a sort of merry-go-round with some people in jail, some people on the street, and some people on trial, but the total impact on the community, although you have some in jail and some on trial, is that the operations go on like they always did?

MR. BARRON: We have a bank robbery a day in Los Angeles—I think it even gets higher. We prosecute them and give them sentences that are pretty good but we still have a bank robbery a day. Should we stop working bank robberies?

PROFESSOR BLAKEY: Would you have more bank robberies if you didn't prosecute them?

MR. BARRON: I don't know. I don't know. I am guessing. But I can't stop working them.

MR. STAFFELD: I am sure if we stop investigating bank robberies we will have more of them.

PROFESSOR BLAKEY: Do you get a feeling that any of the gambling is down from what it was?

MR. BARRON: Yes. We have reports from informants. In Los Angeles it is not hard to go over jurisdictional lines. It is not like New York City where it is all New York City. We have maybe ten police departments concerned with one bookmaking operation because they are situated in locations that the jurisdictions would be multiple. And we see them go down. They may come back in but they will be very small, perhaps five or six people. Because they know what we are doing. They know we are getting people to talk about them. And they keep firing these people and hiring new ones in the hopes they have got our people when they fire them and they reduce. They are afraid. When they are on probation or parole, they are afraid.

PROFESSOR BLAKEY: What is your professional judgment of the impact of this extortion prosecution taking out the leadership structure of the family? What will that do to the family's leadership in Los Angeles?

MR. BARRON: Hurt it.

PROFESSOR BLAKEY: Just while they are in jail?

MR. BARRON: Until they get out and do something else.

PROFESSOR BLAKEY: Do you think when they get out they will be able to reestablish as they were before?

MR. BARRON: Yes, sir, as long as they are alive.

PROFESSOR BLAKEY: Do you get the feeling that maybe some of their sons and daughters aren't going on in the family business?

MR. BARRON: I don't think it would be very attractive to them. I don't know, though.

PROFESSOR BLAKEY: Thank you.

CHAIRMAN ERICKSON: Mr. Westin.

MR. WESTIN: I wonder if you could tell me about the inventory control system as it works in your office. Would you describe physically where the equipment is held and a little bit about your logging procedure just so I can get a picture of how it works and the location?

MR. BARRON: When you say "inventory," first of all, do you mean the tapes we have taken?

MR. WESTIN: I am thinking of all the equipment used for telephone tapping, room bugging.

MR. BARRON: I am not going to be able to answer that as completely as you like and I am not being evasive. But we are a large division and we have an administrative division. And they supervise the handling of that equipment. And all I know is if I have need for three lines I know the equipment is here. I know that Washington sends it out. And I know it is on inventory because everything else I have is on inventory. My chair that I sit in is on inventory and I am sure they've got better safeguards against that equipment.

But I know I can't go and check it out. Even as a supervisor they don't give me that equipment.

MR. WESTIN: In other words, the effective management of the inventory is not in your hands at all, but in the hands of the Administrative Division?

MR. BARRON: That is right.

MR. WESTIN: Therefore, if our Commission wanted to get a picture of the actual working in your office, we would have to have somebody from the Administrative Division describe physically how they store it and what the sign-out procedures are. You don't handle it.

MR. BARRON: I don't handle it. I know where it is stored, sir, but I don't have a key to that room.

MR. WESTIN: Supposing that you are conducting an investigation and there is a location where you have reason to believe from informants or some other source that a conversation will be held for which you want to make a Title III application.

MR. BARRON: Yes.

MR. WESTIN: Would your division make an initial estimate about the feasibility of the telephone tap or room microphone, that is, to see whether the physical layout of the place you want to overhear the conversation in would lend itself to a Title III application, or would you call on a technical expert to make that kind of judgment as to feasibility in that location?

MR. BARRON: No, I would make that judgment.

MR. WESTIN: You would?

MR. BARRON: Yes.

MR. WESTIN: Does that ever entail your testing equipment?

MR. BARRON: Never.

MR. WESTIN: To see whether it would work?

MR. BARRON: You mean an entry into that location?

MR. WESTIN: Not entry, but supposing you have the possibility of using a parabolic microphone—

MR. BARRON: I don't know what that is.

MR. WESTIN: A long-distance mike, a shotgun mike, whatever you call it. Maybe this never occurs but if so I would like to know—do you have reason to believe people are going to be sitting on a park bench or meeting on a street corner and you would like to overhear, with a court order, the conversation?

MR. BARRON: Do we ever test it before we get permission?

MR. WESTIN: Does that mean that sometimes you don't go to request an application because you doubt the technical capacity?

MR. BARRON: No. We don't always have sound studio productions, you know. There are radios

blasting and air conditioners on and it is difficult to learn. I would like to be able to set the stage, but sometimes we don't have the best of conditions—not caused by the equipment, but caused by the very cautiousness of the subjects. They turn the radio up, the television is blaring and they are whispering. And that is pretty hard to make. But we don't test first to see, no.

MR. WESTIN: In your office who would receive any kind of complaint from the public, an allegation that their telephone had been tapped by the FBI?

MR. BARRON: Well, we have a system in our office and I think all offices do—we have complaints—people assigned to complaints. They would be most likely to get it and they could refer it to the desk which handles that type of thing which is not myself, and he could take the complaint.

MR. WESTIN: Are you ever involved in checking out a complaint like that?

MR. BARRON: I don't work that.

MR. WESTIN: In other words, you are not consulted in some sense because they might say—

MR. BARRON: I am not consulted because there is another squad that works it.

MR. WESTIN: That would be true even though the complaint might state that it is the people investigating organized crime?

MR. BARRON: Oh, if it were organized crime I would know about it—anything, even if they said it. Yes, they would channel that down to me. But it is like the fellows that work, say, major thefts, securities—a normal security case I wouldn't know of.

MR. WESTIN: Let's see if I can get my question so my own mind is clear. I am thinking of a situation where somebody from the public complains to your office, to the local FBI, that they believe their wire is being tapped, and they said that because they believed that they are thought by the FBI to be a member of the local organized crime family their wire is being tapped or there is surveillance. I just want to understand how that would be handled in your office.

Would they check with you to say, "Look do you have any taps"?

MR. BARRON: Under those conditions they would ask me if I have any Title III's going with respect to Joe.

MR. STAFFELD: Sir, could I rephrase your question. You are asking if a citizen came off the street and alleged that an agent were running a tap on somebody, what would happen to this allegation in the Los Angeles office?

MR. WESTIN: That is my question.

MR. STAFFELD: I am sure in Los Angeles we have a Complaint Agent who receives complaints

from the citizens who call in or walk in off the street. And they make known their complaint to us. This Complaint Agent will write up the complaint—it is in written form—and channel it to the supervisor who would handle that investigation. In this case we would call it a IOC case, which is an Intercept Oral Communications.

These are specialists themselves and they would work that case. The case would not be referred to Mr. Barron for his overseeing, knowledge, or what have you. It would be handled by the IOC desk.

Does that help?

MR. WESTIN: Yes. I guess I need just one more factual reply.

Do any of you know whether there have been such complaints since the passage of Title III, directed not to wiretapping by other people, private eyes and local and state police, but have complaints been received anywhere saying that FBI agents are illegally wiretapping which is then investigated by your Complaint Division?

MR. STAFFELD: Mr. Cleveland and Mr. Kelly and I are from Headquarters and know of none. The gentlemen from the field offices can speak for themselves.

MR. BARRON: I know of none.

CHAIRMAN ERICKSON: Nobody at the table has heard of any?

[Negative response.]

MR. WESTIN: Thank you very much.

CHAIRMAN ERICKSON: Just one question. What do you do when you do obtain your Title III right to intercept and the person that is being intercepted has the belief that he is being intercepted and contacts the phone company to find out? How do you protect your security?

MR. BARRON: They won't tell them.

CHAIRMAN ERICKSON: And that is their instructions pursuant to—

MR. BARRON: Well, the order.

CHAIRMAN ERICKSON: The order?

MR. BARRON: Yes. They are ordered not to.

CHAIRMAN ERICKSON: Any further questions?

MR. WESTIN: Mr. Chairman, I wonder if I could just follow up on your question?

Are there some phone companies that take the view that they will not affirmatively state there is no wiretap but will give something less than a direct and affirmative answer?

I have heard that some do.

MR. BARRON: I don't know. I only know of Los Angeles.

MR. WESTIN: I have heard some feel threatened by the situation and say—

PROFESSOR BLAKEY: Will we have representatives of AT&T?

MR. HODSON: The third week in June.

CHAIRMAN ERICKSON: I think we can develop that further, then.

Does that complete the questioning?

MR. WESTIN: Yes.

CHAIRMAN ERICKSON: Thank you very much. We are indebted to you, Mr. Barron, for coming out from sunny California to the Capital city.

MR. BARRON: Thank you. It has been a pleasure.

CHAIRMAN ERICKSON: And we hope we will see you again.

Your next witness will be Benjamin P. Grogan, Special Agent and Supervisor, Organized Crime Division, Federal Bureau of Investigation, Miami, Florida.

You have previously been sworn.

TESTIMONY OF BENJAMIN P. GROGAN, SUPERVISOR, ORGANIZED CRIME DIVISION, FEDERAL BUREAU OF INVESTIGATION, MIAMI, FLORIDA; ACCOMPANIED BY ALVIN A. STAFFELD, INSPECTOR, AND JOHN E. KELLY, JR., INSPECTOR, FEDERAL BUREAU OF INVESTIGATION

CHAIRMAN ERICKSON: Mr. Cook.

MR. COOK: Thank you, Mr. Chairman.

Mr. Grogan, your present capacity is what?

MR. GROGAN: I am Supervisor of an organized crime squad in Miami, Florida.

MR. COOK: How many agents do you have under your supervision and control right now?

MR. GROGAN: I have one of the squads that work organized crime and I have 13 agents.

MR. COOK: Thirteen agents?

MR. GROGAN: Yes.

MR. COOK: Is there another organized crime squad in Miami?

MR. GROGAN: Yes, we have two more organized crime squads in Miami. One has the same number of agents and another one has eight agents.

MR. COOK: Are these squads divided up according to offenses?

MR. GROGAN: Two of the squads are divided up according to offenses and one squad handles another county which is the Fort Lauderdale area.

MR. COOK: What offenses does your squad handle?

MR. GROGAN: We handle all gambling violations, violations of interstate transportation involving obscene matter, the Mann Act, and also the Interception of Communications Act.

MR. COOK: And what is the area of greatest activity?

MR. GROGAN: The gambling.

MR. COOK: How many orders has your office obtained since 1968?

MR. GROGAN: We have had 82 installations which involve 25 cases. That would be approximately 25 court orders. All of them were on telephone interceptions. And all of them were for gambling with the exception of, I think, three microphones which were extortion—Shylocking cases.

MR. COOK: What was your background before assuming the job as supervisor of the Organized Crime Division?

MR. GROGAN: I have been in Miami for eight years, four of which I have been Supervisor of Organized Crime. Before that in Miami I worked organized crime. Eleven of my 13 years as an agent, I have been involved in the technical aspects of electronic interceptions in addition to my other investigations.

MR. COOK: By "technical aspects," you are referring to—

MR. GROGAN: The installation of interceptions.

MR. COOK: While you were working in the Technical Section, what would your duties characteristically consist of? What types of things?

MR. GROGAN: Well, I had cases to work like other agents but whenever opportunity arose for the installation of any type of electronic interception, I was one of the agents called upon to make the interception. And I also maintained custody, inventory, of all the technical equipment in our Division, the Miami Division.

MR. COOK: Have you received any instruction in this phase of your work?

MR. GROGAN: Yes. I have received technical instructions—technical training, rather, for this type of work.

MR. COOK: Where was that training received?

MR. GROGAN: I had about two months of this type training in New York City, and I also had about six weeks of it here in Washington, D.C.

MR. COOK: Does this training cover the installation of oral intercept as well as telephone intercept devices?

MR. GROGAN: Yes, it did.

MR. COOK: And your work at the same time, I take it, also includes involvement in other phases of investigations, active informant contact and physical surveillances?

MR. GROGAN: Yes. I supervise the investigation of these gambling cases and the other cases I mentioned, as well as the supervision and installation of the interceptions.

MR. COOK: How active a role are you able to take in the installation of the monitoring devices

themselves? Do you do this or do other agents do it?

MR. GROGAN: I do it and I also have other agents who do it. There are a couple others in Miami that make the actual connections, do all the technical work whenever there is an interception.

MR. COOK: I think you indicated when we visited in the Miami office, that initially you had some difficulties with Southern Bell Telephone regarding installation of the equipment down there.

Can you tell the Commission what the circumstances of that were?

MR. GROGAN: Well, I think it was just because of a matter of time. We couldn't get the installation in as quickly as wanted. It was due maybe to technical difficulties with the cables and pairs. In other words, sometimes we wanted to have a plan to monitor our interception in particular locations, and we had a problem getting vacant pairs. And some of this may have been because the cables and pairs just were not available at those locations.

MR. COOK: Well, as a matter of fact, was it quite frequently that you did not receive the correct cable and pair information from the telephone company?

MR. GROGAN: Frequently we haven't. I don't think there was anything deliberate about it; it is just whenever you have an interception you might have to pick out two wires from a cable of as many as 600 pair. They have to give you the proper color code and cable so you can make the interception. I don't think there is anything deliberate about it; it is just a matter of a problem.

MR. COOK: Then, without the technical background you have, I take it you would be unable to get through the first stages of the intercept because of the situation?

MR. GROGAN: Yes.

MR. COOK: Miami is known as "an open city," I believe, in organized crime parlance.

MR. GROGAN: Yes, that is correct. There are no particular families, as such, like in New York, that control the Miami area. Anyone can come down there and operate.

MR. COOK: What effect does this have on your intelligence gathering? Does this broaden the scope of what you have to learn about if you don't have a stationary object in the form of a local family? Do you frequently have people in transit going back and forth?

MR. GROGAN: This does have some effect on our intelligence gathering in that we have to be much more flexible and maintain constant contact with our sources so that the Bureau will be aware of who is in transit in and out of Miami, as well as those individuals who live in Miami and are involved in organized crime activities.

MR. COOK: You indicated you had approximately 82 installations and 25 orders, so this means in the typical order you would have more than one telephone under surveillance.

MR. GROGAN: Yes.

MR. COOK: What percentage of these have been for violations of 1955?

MR. GROGAN: I would say approximately 85 per cent or 90 per cent for 1952 and 1954 and the rest for 1955.

MR. COOK: So you have had substantial interstate gambling activity in Miami?

MR. GROGAN: Yes.

MR. COOK: What have been the other violations which have been the subject of your intercepts?

MR. GROGAN: The Shylocking has been the other one in which we have utilized a Title III.

MR. COOK: Does Shylocking in Miami take a usurious loan situation or is it a collection of bad debts from unfortunate bettors?

MR. GROGAN: The experience we have had has been the usurious loan situation. And we have had actually professional Shylocks who lend out money. I don't know of any cases where we have utilized Title III as a result of gambling debts.

MR. COOK: Have you been successful in any of your extortion threats?

MR. GROGAN: Yes, we have.

MR. COOK: Have those cases come to trial?

MR. GROGAN: Yes. We had one come to trial and they all received substantial sentences because of the violence that they did use in some of these cases.

MR. COOK: Would you recall the names of the defendants in those cases?

MR. GROGAN: One of the defendants was Gary Bodach and others who were involved in it.

MR. COOK: Did they have any organized crime families?

MR. GROGAN: Yes, we believe from informant information they were involved with the organized criminal element.

MR. COOK: Have you ever used videotape surveillance in Miami for any reason?

MR. GROGAN: Yes, we did.

MR. COOK: And what kind of situation was this?

MR. GROGAN: That was during the conventions, the demonstrations. We used videotape.

MR. COOK: This was non-organized crime?

MR. GROGAN: Right.

MR. COOK: Approximately—excuse me. You may have already answered this. Approximately how many technical agents do you have working for you?

MR. GROGAN: How many technical agents?

MR. COOK: Yes, sir.

MR. GROGAN: There are three.

MR. COOK: Three. And of the three of these, how many are used for installation of equipment? Do you have to utilize all of them?

MR. GROGAN: In most cases we utilize all three, because we have multiple telephones to be connected and there is a lot of technical work to be done on Title III.

MR. COOK: Can you tell the Commission what some of the hazards are as far as installation of telephone lines and equipment? Is this an inside job as far as you are concerned or have you been involved in telephone calls—

MR. GROGAN: Based upon the cable-pair information and the color codes given to us by the telephone company, we connect the subscriber's pair to the leased line ourselves. And these leased lines will either run through our office or to what we call an outside plant, a location that we are going to monitor. And we connect these leased lines up to recording equipment so we can record the conversations and obtain the out-dialed numbers.

MR. COOK: Have you found it impossible to install the necessary equipment because of physical obstacles to climbing the pole or risks you couldn't afford to take?

MR. GROGAN: No, there is no physical obstacle, really. The problems you may have sometimes is there are no cable and pair available where you might want to monitor the surveillance. But we have always been able to overcome it. We have never missed out on the installation of a Title III because of technical difficulties in Miami.

MR. COOK: What are the typical types of oral intercepting equipment that your office uses?

MR. GROGAN: Of oral interception?

MR. COOK: Yes, sir.

MR. GROGAN: Well, we would utilize microphones which are connected to a wire—we call them wire microphones, or radio microphones, either one of the two.

MR. COOK: How does a wire microphone work?

MR. GROGAN: Well, a radio microphone is tuned to a particular frequency which would transmit the conversations in the room to an outside location. It is just like a small radio transmitter—radio microphone. And this is concealed.

A wire microphone is a microphone that is attached to wire and it is necessary usually to lease a pair to a particular plant so you can monitor the microphone.

MR. COOK: Are you familiar at all with—I believe it is called a harmonica bug?

MR. GROGAN: Pardon me?

MR. COOK: The harmonica bug or affinity transmitter.

MR. GROGAN: No, sir.

MR. COOK: The Commission has been informed in the course of exploring technological developments that there is a type of interception device where you dial the number of the phone to be intercepted and apparently by blowing a certain frequency on a harmonica, a series of notes, you can turn that telephone into a monitoring device.

Have you had any experience with that?

MR. GROGAN: No, I have never heard that particular name. You mean for oral interception or for an interception of wire?

MR. COOK: I think it is for the interception of wire communications.

PROFESSOR BLAKEY: It is oral; it is oral.

MR. COOK: Maybe for the time I can throw that question open. Is anyone at the table familiar with that?

MR. STAFFELD: There has been some telephone company research in that area, because there has been some illegal use of telephone lines by—you use a harmonica but others use tuning forks and other devices that do cause this interchange in the computer system. And I am not technically—

MR. HODSON: Mr. Chairman, that is going to be fully covered the third week in June.

MR. COOK: You have access to leased lines in Miami, is that right?

MR. GROGAN: When we have a court order.

MR. COOK: Pardon me?

MR. GROGAN: When we have a court order for an interception, then we can rent leased lines.

MR. COOK: And do you run one of your interceptions to a plant in your office, or do you have the plant removed from the office, or does that depend?

MR. GROGAN: Well, that depends. If the telephones to be monitored are a long distance from our office, then we would rent a plant, an apartment, and run the lease lines to the apartment. If they are in the same telephone exchange as our office, we may utilize our office as a plant.

There are other factors, also. You have to obtain the out-dial numbers in a gambling operation. When you have run your leased pair through several telephone exchanges, the equipment usually won't pick up these out-dial numbers. And so we try to get a plant that is close by.

MR. COOK: Are you responsible for assignment of the manpower to run your wiretap plants?

MR. GROGAN: Yes.

MR. COOK: Approximately how many people does it take to operate a plant, say the average plant indicated would have about three phones?

MR. GROGAN: You have three telephones and it is according to whether the phones are going to be utilized for a particular period of time.

For instance, on a gambling operation—in football season it may only be run in the morning and in the late afternoon. So for each line that is being monitored, you would put an agent on it. That would be three agents there. If there are two shifts, you have to have six agents.

You also have to have the case agent and another agent assisting him, usually, who is totally involved with handling the traffic that comes in. A supervisor would be involved. You would have to have surveillance agents for the subjects to make sure that they are in the location where you are monitoring.

You have the supervisor's time taken up and you have a technical agent on duty all the time, at least on call in case there are any technical problems involved in the plant.

If the plant would be in the office, then we wouldn't have to man it 24 hours a day. If it is an outside plant, we would have to have an agent on duty there 24 hours a day to protect the equipment.

It is hard to give the exact number of agents for the exact number of phones. It would vary.

MR. COOK: Do you also supervise the use of consensual recordings in your office?

MR. GROGAN: Yes, I do.

MR. COOK: What kind of inventory procedures do you use? Is your equipment signed in and out?

MR. GROGAN: Yes, our equipment is on inventory. If an agent needs to use a consensual device to monitor conversations, he would come see one of the agents charged with signing it out, which is one of the three technical agents, and they would sign it out to him. They would install it on the person, if it is a body recorder, themselves.

MR. COOK: I see.

CHAIRMAN ERICKSON: Let's take a five-minute break.

[Whereupon, a short recess was taken.]

PROFESSOR REMINGTON: I think we are ready to resume and Dave Cook has another question or so to ask.

MR. COOK: Mr. Grogan, can you tell us what types of measures are necessary to take for the installation of oral intercept bugs?

MR. GROGAN: For an oral interception you have to make a survey of the premises or location wherein the interception is going to take place. You have to ascertain whether or not it would be technically feasible. If the interception is going to be next to a train depot or some place like that where you couldn't hear anything, all these things have to be taken into consideration.

You have to—after the court order is obtained, you have to find out whether or not you are going to use a wire microphone or a radio microphone. In

our case the wire microphones are preferable because of their fidelity which is much better than radio microphones. Radio microphones are subject to interference because of other radio transmission sometimes or the steel in a particular building.

Then you have to make installation of the microphone, itself. And after the installation of the microphone is made, then you make the necessary connections to your lease lines back to the plant—or you have a plant nearby wherein you could monitor it over the radio frequencies.

MR. COOK: When an installation has to be made on private premises, I assume you are authorized by court order to make whatever kind of entry is necessary in order to install the equipment; is that correct?

MR. GROGAN: Yes.

MR. COOK: Does this generally involve some kind of surreptitious entry?

MR. GROGAN: Yes. If you don't have a key to the location you have to establish other means of entry.

MR. COOK: I see.

Mr. Chairman, that concludes the staff's questioning.

PROFESSOR REMINGTON: Okay. Mr. Westin.

MR. WESTIN: You have described two types of oral interception devices, radio microphones and wire microphones.

Has your office ever used any other kinds of devices such as devices to take sound off vibrating window panes or parabolic microphones to try to listen to a conversation from private premises across the street or something like that? Are there any such examples, in your experience?

MR. GROGAN: Not that I can recall, no. We have only had court orders, as I said, in four cases for these microphones and they were all wire, with one exception.

MR. WESTIN: I see. Is the situation that I have described—maybe the other gentlemen could comment on this—where it might be perilous to get on premises because of watchdogs on a private estate or something like that, in which you can obtain a court order on the theory of probable cause—does it ever arise that that kind of situation has come up?

MR. GROGAN: You mention different things, telephone and microphone. Telephone is no problem.

MR. WESTIN: I meant only oral conversations. I am not talking about telephone conversations.

MR. GROGAN: No, it hasn't come up in Miami.

MR. STAFFELD: I know of none.

MR. WESTIN: You mentioned videotaping political demonstrations.

MR. GROGAN: That is correct.

MR. WESTIN: Was it used to monitor the public or private?

MR. GROGAN: I wasn't supervising that. It was mainly to observe the demonstrations of the public.

MR. WESTIN: It took place on public streets?

MR. GROGAN: Public streets.

MR. WESTIN: As far as you know, it was not the placement of a video device in a private office or a private home?

MR. GROGAN: No, it was not.

MR. WESTIN: Have you ever had occasion to ask the telephone company to provide you with space on their own premises for listening or do you always go to your own office or to a leased listening post somewhere near the place where the telephones are?

MR. GROGAN: We always go through our own office or our own plant.

MR. WESTIN: In your office is the physical maintenance of the equipment under your jurisdiction?

MR. GROGAN: Yes, it is.

MR. WESTIN: Could you describe to me the techniques of physical control, inventory records, and so forth, used?

MR. GROGAN: For every piece of equipment we maintain an inventory card by type of equipment and serial number. A copy of this card is also maintained at Bureau Headquarters as to what equipment we have. Whenever a piece of this electronic equipment is to be used, it is usually checked through me or one of the other agents who handle this matter and we charge it out.

In most instances, in fact nearly all, one of the technical agents will accompany the equipment to be utilized.

MR. WESTIN: Does the card system mean that you can tell by some kind of case number or case number identification for each piece of equipment over a period of time what case that piece of equipment was used on? Is that the way the card system works? Or is it checked out to an agent by name?

MR. GROGAN: It would be checked out to the agent by name. We don't maintain it by case.

MR. WESTIN: Have you had any experience in your office with efforts to develop tapes that are not—maybe I should save that for the technical discussion.

That is all. Thank you, sir.

PROFESSOR REMINGTON: Mr. Pierce.

MR. PIERCE: I have no questions.

PROFESSOR REMINGTON: Judge Shientag.

MS. SHIENTAG: No questions.

PROFESSOR REMINGTON: Mr. Blakey.

PROFESSOR BLAKEY: Let me just ask you a general question. I think maybe I know the answer

or can infer what your answer might be from what you have said.

I take it the type of equipment that you are using is not 1984, just a straight radio or a straight wire bug?

MR. GROGAN: Yes.

PROFESSOR BLAKEY: Do you have any 1984 type of equipment?

MR. GROGAN: No, we don't in Miami. If we had need for that we could get it from Bureau Headquarters.

PROFESSOR BLAKEY: Is it available to you, that is, sophisticated equipment?

MR. GROGAN: If a sophisticated piece of equipment were necessary we could get it from Bureau Headquarters.

PROFESSOR BLAKEY: Do you have occasion to use it? Or are most situations easily handled either by a wiretap or wire bug or radio bug?

MR. GROGAN: I have found in my experience the simpler the equipment, the better the fidelity and everything.

PROFESSOR BLAKEY: Have you had problems with malfunctioning equipment?

MR. GROGAN: No, we maintain our equipment. We keep it in working order and we maintain it in good shape. There may be something once in a while will happen to a piece of equipment that can be fixed, but our equipment is maintained.

PROFESSOR BLAKEY: Do you have problems with, not malfunctioning equipment, but situations that interfere with surveillance—radios—airplanes flying overhead?

MR. GROGAN: That happens, right.

PROFESSOR BLAKEY: Do you have any technical means of getting around that kind of problem? I am talking about a phone now.

MR. GROGAN: On the telephone—

PROFESSOR BLAKEY: It is easy because if you can't hear it, neither party can hear. But on a bug—

MR. GROGAN: On the telephones we have had hardly any technical difficulties.

PROFESSOR BLAKEY: How about the bugs?

MR. GROGAN: The bugs on occasion we have had it—when someone turns on the air conditioner or radio next to it, and it is very hard—very difficult then to hear what is being said. We found this in instances of consensual monitoring where the victim in a particular case is to meet the subject and they may, instead of going to the car for the conversation—the subject may say, "Let's go into this restaurant." Microphones don't have the ability of the human ear to just hear the conversation from one person to another. It picks up all the ambient noises.

PROFESSOR BLAKEY: What I am trying to get at is that there is a kind of feeling among people that you have a 1984 capability where you can pick up anybody's conversation in any room anytime and in high fidelity. Does that reflect what the practical experience in the street is?

MR. GROGAN: If the high fidelity situation is in the room, you can pick it up. If you have a situation in the room where the baby is crying or everybody is shouting or whispering—

PROFESSOR BLAKEY: What is the more common situation?

MR. GROGAN: The more common situation is, in my experience with microphones, that we've got good fidelity on them, especially wire.

PROFESSOR BLAKEY: Thank you.

PROFESSOR REMINGTON: Chief Andersen.

CHIEF ANDERSEN: I just have a couple of questions.

What is the telephone company in your area?

MR. GROGAN: Southern Bell.

CHIEF ANDERSEN: Will they make the final hook-up for you?

MR. GROGAN: No, we make all the hook-ups to the leased line. It is necessary for the phone company—if we go through more than one telephone exchange with our leased line, it would be necessary for the phone company to put in amplifiers in the central office of the telephone company so that we could be able to hear the conversations back at our plant.

CHIEF ANDERSEN: Do you make the actual physical connections yourself?

MR. GROGAN: We make the actual physical connection of the leased line to the subscriber's line, yes.

CHIEF ANDERSEN: Will they give you a central office hook-up?

MR. GROGAN: No.

CHIEF ANDERSEN: May I have your understanding of why they won't do this?

MR. GROGAN: No, I am not familiar as to why they won't do it, but I have been told they won't do it in the Miami area.

CHIEF ANDERSEN: They won't make the final hook-up for you? They will not connect a complete tap for you?

MR. GROGAN: No, this is by our own preference. We would rather make our own hook-up ourselves. Hooking up a leased line is not just like connecting a telephone. It is something that has to be done with some degree of security.

If you have, for example, a bookmaker in there running his business at ten o'clock in the morning and the telephone man goes out at ten o'clock and starts interfering with his communications, he is

going to know that somebody is fooling with his telephone lines. We go out and make sure that the line is secure, there is no one using it, and we make the connections. We also check our connections. It is not the usual type of connection. We make sure there is no trouble—what we refer to as trouble—so when he does try to use his phone he won't find it is out of order.

We make these checks. We also check so that we can testify in court that we are on the right line.

CHIEF ANDERSEN: But a central office hook-up would eliminate all that?

MR. GROGAN: Yes, it would.

CHIEF ANDERSEN: But they just won't do it?

MR. GROGAN: We haven't asked them, but they have told us, "We won't do it."

CHIEF ANDERSEN: You haven't asked them, but they told you no; is that it?

MR. GROGAN: Right.

CHIEF ANDERSEN: The reason I am asking those questions is we have all kinds of telephone companies and we have had all levels of "how to do it", and I am trying to find some common level in there that meets anybody's reasonable satisfaction.

MR. GROGAN: Our leased lines that run through the central office—it is necessary for them to hook into the central office.

For instance, if we make a connection of a leased line to a subscriber's line, our leased line and the subscriber's line may run back to the central office. There at the central office our leased line is in the hands of the phone company and it is going to be necessary for them to connect other leased lines to that so we can monitor it in a distant monitoring office.

CHIEF ANDERSEN: That is to get your power boost?

MR. GROGAN: Power boost and also make the necessary connection.

CHIEF ANDERSEN: Do you have any problems with them on pen registers? Do you use pen registers?

MR. GROGAN: We use pen registers in all our Title III's on gambling. We haven't had occasion to use a pen register by itself.

CHIEF ANDERSEN: Do you use a court order for pen registers?

MR. GROGAN: We obtain a court order when we get a pen register.

CHIEF ANDERSEN: I won't go into the technicalities between Rule 41 and Title III.

But you have experienced no difficulties on this? Do you get them in advance of the Title III?

MR. GROGAN: No, we obtain the court orders for the pen registers at the same time we get the order for the interception. We do it at the same time.

PROFESSOR REMINGTON: I might follow up on that. We had some testimony yesterday on pen registers and there was an indication that they were secured under Rule 41 rather than under Title III. Is that your experience?

MR. GROGAN: We haven't had that experience in Miami because we haven't utilized it. I understand you can get a pen register under Rule 41, like you would a search warrant.

PROFESSOR REMINGTON: But you haven't had occasion to do it?

MR. GROGAN: No.

PROFESSOR REMINGTON: Okay.

Is there anything else the Commission should know this afternoon?

MR. GROGAN: No.

PROFESSOR REMINGTON: We very much appreciate your being here and thank you very much.

I guess we are going to hear from Mr. James Esposito. I assume you have already been sworn?

MR. ESPOSITO: Yes, sir.

PROFESSOR REMINGTON: We are happy to have you here and I think Mr. Cook is going to start questioning.

**TESTIMONY OF JAMES ESPOSITO,
ASSISTANT SUPERVISOR,
ORGANIZED CRIME DIVISION,
DETROIT, FEDERAL BUREAU OF
INVESTIGATION; ACCOMPANIED BY
ALVIN A. STAFFELD, INSPECTOR,
AND JOHN E. KELLY, JR.,
INSPECTOR, FEDERAL BUREAU OF
INVESTIGATION**

MR. COOK: Mr. Esposito, what is your present position?

MR. ESPOSITO: I am a relief supervisor in the Detroit office of the FBI.

MR. COOK: And what does your work consist of primarily?

MR. ESPOSITO: I am assigned to an organized crime squad which handles illegal gambling business.

MR. COOK: And do you do any work besides that on illegal gambling?

MR. ESPOSITO: That is the bulk of my work. Occasionally—we have five squads in my office that handle organized crime, and necessarily, because of the types of people that we are dealing with, we occasionally will deal with other violations. But the vast majority of my work deals with the IGB statute.

MR. COOK: Do you have any idea of how many IGB investigations you have been involved with as an agent?

MR. ESPOSITO: Personally?

MR. COOK: Yes.

MR. ESPOSITO: Approximately 50.

MR. COOK: And you have been the affiant on how many Title III affidavits to the best of your recollection?

MR. ESPOSITO: Five.

MR. COOK: And you were also a case agent, I believe, in at least one Title III prosecution, were you not?

MR. ESPOSITO: Yes, sir.

MR. COOK: What was the name of that case?

MR. ESPOSITO: *U.S. v. Orlando James Vigi*.

MR. COOK: Were you the case agent at the investigative stage of that case as well?

MR. ESPOSITO: Yes, sir. I had that case from its very inception.

MR. COOK: Can you describe in outline form how that case took shape from the inception to Title III work and the indictment stage?

MR. ESPOSITO: Yes, sir. That case was initiated on the basis of informant information which we received. I developed an informant who identified himself to me as being a part of the large bookmaking operation. In contacting this individual on an almost daily basis, further information was gained from him and also he was given direction by me as to certain types of information that we felt were needed.

That information was presented to the Strike Force attorney and a decision was made approximately two months after the initial information was provided that we should apply for a Title III order.

Subsequently an affidavit was prepared and it was approved and a Title III installation was made. And subsequently 40 people were indicted. Following this we had 36 convictions.

MR. COOK: Was there more than one order signed in that case?

MR. ESPOSITO: Yes, sir, there was. There were two orders and one extension of the first order.

MR. COOK: Do you recall how many different telephones that covered?

MR. ESPOSITO: There were a total of ten telephones, seven on the first order and extension and three on the subsequent order.

MR. COOK: Approximately how many agents were working on this case under your direction at any given time?

MR. ESPOSITO: We had one agent assigned to each telephone during the monitoring. In addition to that, we had approximately 15 agents who were involved in physical surveillance. And there were, in addition to that, probably four or five agents assisting me with the administrative tasks of keeping up with the paper work.

MR. COOK: Can you describe in detail what this paper work includes?

MR. ESPOSITO: Yes, sir. During the course of the monitoring we had one agent assigned to each telephone. When the equipment is activated either by an incoming or outgoing telephone call, the agent maintains what we describe as an agent's log. On that he will record the time of the interception, when the machine is turned on, the recording device is turned on to intercept the conversation. He will initial that form and later identify who the monitoring agent was.

In addition to that he will, as the conversation is being intercepted, make a summary of the gist of the conversation, important comments that are made, whether or not a meeting will take place, something that will alert me as a case agent to a certain action I must take, whether it be follow-up surveillance or, if it is an outgoing telephone call, whether or not a subpoena should be prepared for the subscriber—things of this nature.

That log is maintained on a daily basis. It is turned over to me as the case agent at the close of each day's activity.

In addition to that, we also have a log which we identify as an activity log. On that we record at the end of the day's actions the number of telephone calls which are intercepted and in the judgment of the monitoring agent how many of those calls would be classified as violations of the statute, how many of those calls would be considered as personal, or how many of the calls would be in a classification we describe as "Other." And that would include calls which might be busy signals or incompleting dial, things of this nature.

In addition to those two logs, we maintain a third log which we call a posting log. And on that log we record all of the outgoing telephone numbers which we pick up from the pen register device.

MR. COOK: Now, as the agent in charge, are you responsible for the review of the agent's log for each telephone?

MR. ESPOSITO: Yes, I am, and that is done on a daily basis.

MR. COOK: And is it your responsibility then to scan these logs and select the conversations that either the monitoring agent or you deem to be especially pertinent?

MR. ESPOSITO: Yes. As a matter of fact, at the inception of the monitoring, the monitoring agents are given certain directions by me and my supervisor. And they are told to key certain of the conversations to our attention. They will star the log to bring certain things to our attention that we may not pick up on a minute-to-minute basis, but we may see the next morning.

And those conversations are reviewed by me the following day and normally they are assigned to be transcribed.

MR. COOK: Would you consider the Vigi tap to be an active tap or not very active or very busy?

MR. ESPOSITO: I would consider it to be a very busy tap. We were on those phones for approximately 20 days and during the course of those interceptions we intercepted in excess of 4,000 telephone calls, and the vast majority of those were violation calls.

MR. COOK: Now, this means that you would have to look at approximately how many starred entries in agents' logs as far as pertinent conversations recorded each day?

MR. ESPOSITO: Well, it would vary, but probably I would say 10 or 15 conversations which the monitoring agent felt were especially pertinent.

MR. COOK: And were you able to transcribe these on a daily basis or was the manpower demand just too great?

MR. ESPOSITO: The transcription would begin almost immediately. On my squad we had 15 agents and if we have a situation where we are utilizing Title III, the supervisor will make a decision as to manpower. Certainly he will assign one agent to each telephone, but in addition to that he will also assign certain individuals as their workload permits to do verbatims which would normally start immediately. As the case agent, if my time permits I will do them as well.

MR. COOK: In what form are these verbatims prepared at the time for working purposes?

MR. ESPOSITO: We put a cover sheet on them, a work sheet. They are done in longhand. The agent who transcribes them will identify himself to me on the sheet. He will identify the parties, if they have been so identified in the call. And then he will proceed to transcribe the call. We assign certain terminology to the entries. For instance, we use the code PCM, which would be "Person Calling Male" or "Person Answering Male," "PAM," or substitute "F" for "Female" as prefixes to the various conversations.

MR. COOK: Do you duplicate the tapes to have working copies of the tapes as well as the originals?

MR. ESPOSITO: The tapes are duplicated. We make a working copy of the original the morning following the preceding day's monitoring of the telephone.

In addition, we also make Xerox copies of the handwritten log the agent has maintained for the preceding day so I have a working copy on which I can make notes to myself and to other agents who are working the case.

We maintain the original logs with the original tapes. They are locked in vaults which only my supervisor and the special agent in charge of our office have access to.

MR. COOK: What kind of contact do you maintain with the supervisory attorney during this time?

MR. ESPOSITO: Almost daily contact, and beyond that sometimes it is hour-to-hour contact. We advise him of pertinent activities which we have determined through our installation. But at least every day we make contact with him, either by phone or personally. And more than likely it would be several times during a given day.

MR. COOK: Now, it takes you about how long to set up the monitoring operation after the order has been signed?

MR. ESPOSITO: Are you speaking with respect to placing the recording devices, the tape recorders and so forth?

MR. COOK: Let's say it is Wednesday at three o'clock and you have just gotten the order signed. How long would it ordinarily take you to have the machines operative reporting calls from the subject telephones?

MR. ESPOSITO: Well, it varies. We will immediately serve the order on the telephone company. If we are fortunate, by the next day we can be in operation. There have been situations where it has taken several days because of technical difficulties, to get the equipment in an operative condition.

MR. COOK: And you said that there was extension of orders in this case. How long were the original orders?

MR. ESPOSITO: Twenty days.

MR. COOK: Now, you have to start making preparations, I take it, for preparation of probable cause for your extension affidavit; is that right?

MR. ESPOSITO: Yes, sir.

MR. COOK: Do these have to be done contemporaneously with the preparation of the agents' logs and duplication of tapes?

MR. ESPOSITO: Yes, sir. And approximately about the fifth day of the installation we will begin to have a feel for the operation, for the illegal gambling business, if you will, as to the identity of the participants. And we will begin to consider extension at that time, based on how we feel the case is going.

This, of course, is a determination which the Strike Force attorney makes, but that is another reason why the verbatim transcription will start almost immediately, because oftentimes at least excerpts from intercepted calls will be used and incorporated into the extension affidavit.

MR. COOK: You also, I take it, by means of the pen register device and the use of names in monitored calls, are able to identify certain persons as being participants in these conversations?

MR. ESPOSITO: Yes sir, that is correct.

MR. COOK: Do you have any procedures as far as paper work is concerned in terms of classifying persons who are intercepted, identifying them?

MR. ESPOSITO: Yes, sir. We provide the Strike Force attorney with lists of individuals who have been identified as persons named in the order, and those who have been identified who were not named in the order but who are participants in the illegal gambling business, and also the identity of other persons who are not participants in the illegal activity.

MR. COOK: In other words, I take it some persons are intercepted on these calls before the determination can be made whether the call is a so-called violation call or not?

MR. ESPOSITO: Would you repeat the question, please.

MR. COOK: I take it some persons' conversations are intercepted and recorded before a determination can be made that that call is incriminating or not pertinent?

MR. ESPOSITO: Not exactly. The monitoring agent in gambling-type situations will know, based on his experience, what to listen for. If it is obvious to him that the conversation is not related to what we are looking for based on the order, he will turn the recording device off.

MR. COOK: Now, if you get an outgoing call to a residence at the early stages of the interception before you are familiar with all the participants, I think you have some idea of who is involved on the basis of your informant information, and there are some people who are going to get picked up who are ultimately going to be determined not to be involved in the gambling business; is that right?

MR. ESPOSITO: Yes, that is correct.

MR. COOK: Do you keep any record of the outgoing calls?

MR. ESPOSITO: Yes, we do, in the posting log which I mentioned earlier. All outgoing telephone calls are maintained by number in numerical order in our posting log.

MR. COOK: Do you subpoena the numbers of outgoing calls to determine who the subscribers are?

MR. ESPOSITO: Yes, sir.

MR. COOK: Is there any further record kept of the names of the subscribers once the subpoena is returned?

MR. ESPOSITO: As to those persons that have been positively identified, as I mentioned earlier, a list is given to the Strike Force attorney with their identities. In addition to that we prepare cards which we maintain in our office as to the identity and also provide a copy to the Bureau Headquarters, of that individual's identity.

MR. COOK: For the ultimate purpose of notifying intercepted persons, the statute gives this discretion by letter, but I take it as a practical matter it is something the supervising attorney and the agent, but primarily the attorney, has to determine on the basis of the evidence contained on the recordings; is that right?

MR. ESPOSITO: Yes, sir. In our Division in Detroit the Strike Force attorney will, after being provided with lists of persons who have been identified, come back to us say, "It is up to us to send registered letters notifying certain of the people on the list."

And the criteria he uses are those persons named in the order, those persons he feels will be ultimately indicted, and in addition to that, witnesses who would be called at some future time.

MR. COOK: Once you have concluded the interception stage of the investigation, do you prepare any kind of prosecutive memorandum or case report which summarizes the results of the interception?

MR. ESPOSITO: Yes, sir. When the monitoring has ceased we will then begin to analyze in greater detail all the verbatim conversations that we have. And at that point in time we have pretty much identified those participants that we feel ultimately will be indicted. And at that point a prosecutive memorandum is prepared by me for the Strike Force attorney for his review. And it includes in that certain excerpts from pertinent conversations and so forth.

MR. COOK: Now, what steps do you take to prepare the contents of the recorded calls for use as evidence at trial?

MR. ESPOSITO: In the trial I had with respect to *Vigi*, I sat down with the Strike Force attorney after my review and I said to him, "These are the persons that we have identified and they were obviously involved in the conspiracy and in the substantive violation."

He directed me then to put together a composite tape recording with selected calls which involved all the participants that we intended to indict.

There were in the composite tape we used approximately 90 telephone conversations. And, generally speaking, we had between five and ten conversations per subject with one exception. For Mr. *Vigi* we used over 20. The reason we used that many with respect to him was because we were very fortunate in that he contacted most of the participants. Those telephone calls lent themselves toward showing violations of the elements of crime.

MR. COOK: Was a composite transcript also prepared?

MR. ESPOSITO: Yes, it was.

MR. COOK: And how was this presented to the jury?

MR. ESPOSITO: Each juror was furnished a copy of the transcript which verbatimized the composite tape. The judge had a copy. Counsel for the defense had a copy. And they were allowed to use that as an aid in listening to the tape recordings.

MR. COOK: Let me back up just a minute here.

There is a discovery stage occurring at the postindictment process, pre-trial. What provisions are made for defense attorneys and defendants to listen to the tapes, or to inspect the tapes to determine their accuracy, obtain whatever other information they may wish from the tapes?

MR. ESPOSITO: The Strike Force attorney, after the defense counsel has filed appearances, will direct me to arrange for appointments to be made with the various defense counsel, so they may come in and listen to telephone calls. They had previously been furnished with Xeroxed copies of the agents' logs.

And the way we do it in Detroit to save time, we will ask the defense counsel to advise us by phone call which ones he would like to listen to with respect to his client, so that we may have an opportunity a day or so ahead to have those ready for him.

MR. COOK: Have you found the defense counsel ordinarily are quite diligent in listening to these calls, or is their response less than impressive?

MR. ESPOSITO: I think it varies. Some defense counsel will listen to every phone call. They may listen to 50 or 60 phone calls and make several appointments to come back if their appointments permit. Others have never appeared to listen to calls prior to trial.

MR. COOK: Out of the 40-some defendants, did any plead?

MR. ESPOSITO: Yes, 25 entered pleas and nine were convicted.

MR. COOK: And the other six were dismissed or acquitted, I take it?

MR. ESPOSITO: Yes, that is correct.

MR. COOK: Were you able to assess what kind of effect, if any, this had on the Vigi gambling operation?

MR. ESPOSITO: Yes, we have. We know from follow-up informant information that we put Mr. Vigi out of business. He appealed to the 6th Circuit and that appeal was denied within the last two weeks. But in the interim period since his conviction we know he has not been active in the illegal gambling field.

MR. COOK: I see.

Just one further thing.

How did you accomplish the identity of the defendants by their voice on the telephone?

MR. ESPOSITO: Well, the first and probably the most common was to get the outgoing telephone subscriber. And then we will arrange by physical surveillance to have, if possible, overhears of that particular subject. The overhear agent would then come back and listen to the monitored tape to make a determination whether or not that was the same individual.

In addition, we would make—if the situation presented itself, we would make pretext telephone calls to the individual we believed was the one who had been monitored.

In addition to that, many of the people we have intercepted had previously been interviewed by the FBI. We would review our files and have the agent who interviewed him come in and listen if possible to the monitored conversation.

MR. COOK: Did you have any serious challenges by defense counsel as to the accuracy of your voice identification by agents?

MR. ESPOSITO: During the Vigi trial that was one of the major contentions, as to the accuracy of voices. However, in each and every instance the judge overruled their objection and allowed us to use the methods that we did.

MR. COOK: I see.

Mr. Chairman, that concludes the staff's questioning.

PROFESSOR REMINGTON: Judge Shientag.

MS. SHIENTAG: No questions.

PROFESSOR REMINGTON: Chief Andersen.

CHIEF ANDERSEN: No questions.

PROFESSOR REMINGTON: Mr. Blakey.

PROFESSOR BLAKEY: Do you have liaison with the Detroit Police?

MR. ESPOSITO: Yes, we do.

PROFESSOR BLAKEY: Do they take wiretap evidence?

MR. ESPOSITO: No, sir, they don't. I should back up a minute and say we have a limited liaison with the Detroit Police Department at this time.

PROFESSOR BLAKEY: If you had a gambling case where you only picked out 25 of 100 possible defendants, do you have any set procedure whereby you turn over the other 75 to the Detroit people? The Bureau has a normal program of disseminating information to the local people. The annual report is sprinkled with the number of disseminations and numbers of seizures based on them. Does that include wiretap information?

MR. ESPOSITO: Well, the dissemination is made by the Strike Force attorney with respect to the Title III evidence he gets.

PROFESSOR BLAKEY: So if he doesn't disseminate it, it doesn't get disseminated?

MR. ESPOSITO: That is correct.

PROFESSOR BLAKEY: The reason I ask this is we have testimony in the record that the Strike Force in Detroit, in the drug area, has been so overburdened with work that they have a hard enough time trying the cases without disseminating to the locals the narcotic information. And apparently there is good narcotic information that they were not able to prosecute that was simply never turned over.

And I am trying to figure out whether the same thing is true in areas where you are working.

And I take it it is not being given, because you are not passing it on.

MR. ESPOSITO: Well, not in every instance we are not passing it on. In those situations where we have not been able to make a Federal case—and this would be with the concurrence of the Strike Force attorney, obviously—he will direct us to turn over certain information to the locals to execute search warrants or what have you.

PROFESSOR BLAKEY: Have you ever testified on Federal wiretaps in a State case?

MR. ESPOSITO: No, I have not.

PROFESSOR BLAKEY: Are you aware of anybody in Detroit doing that?

MR. ESPOSITO: No, I am not.

PROFESSOR BLAKEY: Mr. Staffeld, are you aware of any situation in the organized crime program where Federal wiretaps have been introduced in State cases?

MR. STAFFELD: We have turned over whole cases. I think it has been done a couple of times in the South. And Ben says he has done it.

PROFESSOR REMINGTON: Have you had problems with the State courts presenting it?

A VOICE: No, they were presented to the District Attorney and they took it before the court?

PROFESSOR BLAKEY: This would be Gurstein in Miami?

MR. GROGAN: Yes.

PROFESSOR REMINGTON: Florida has a wiretap statute?

MR. GROGAN: Yes.

MR. STAFFELD: We had a case in Tennessee—do they have one?

PROFESSOR BLAKEY: They don't have a statute.

MR. KELLY: No Title III.

PROFESSOR BLAKEY: Do you ever have occasion to disseminate information where you get information on a wiretap of another occurrence that you know immediately was going to happen?

MR. ESPOSITO: Yes, we have.

PROFESSOR BLAKEY: With what kind of results?

MR. ESPOSITO: I would rather pass on that at this time. We have a situation which is currently ongoing and I would rather not get into it.

PROFESSOR BLAKEY: How frequently does it occur when you are in on a gambling tap you get information on unrelated things?

MR. ESPOSITO: It is the exception rather than the rule in my experience—very infrequently.

MR. KELLY: I might mention one case—I don't know if it has been adjudicated, but it is in point here. One office picked up some information that an armed robbery was going to take place. We notified the local authorities—and of course it took them some time to get going. And we had our own surveillance team on these people—we knew it because it was on a conversation—and surveilled the location where they were going to commit the armed robbery.

PROFESSOR BLAKEY: I have no further questions.

PROFESSOR REMINGTON: Mr. Esposito, is there anything else you think we ought to know today?

MR. ESPOSITO: I don't think so.

PROFESSOR REMINGTON: All right.

We have from General Hodson a question to clarify an earlier question that was asked this morning.

MR. HODSON: This question will probably be addressed to the Headquarters complement.

This morning Professor Westin was talking about different rules with respect to different criteria, if you will, as to when you seek a Title III wiretap, what kind of case is important enough. And he had indicated he had heard in certain areas of the United States you could get a Title III wiretap for a Mom and Pop gambling operation whereas in other parts of the United States they would never get a wiretap for such a case.

I was wondering if you would tell me whether in the Federal system your review procedures establish any quality control with respect to criteria, for when is a case important enough to warrant a Title III tap?

MR. CLEVELAND: Yes, sir. We always have a quality control. And I believe I said this morning that we specifically avoid Mom and Pop operations or the little old lady at the candy store. We are not interested in those cases because we don't feel that they are quality cases.

However, there are different areas of gambling cases. A gambling case in Mobile, Alabama may be considered very important, and some crooks who are involved there may be deemed to be a quality case by the United States Attorney who is interested in that particular ring being broken up,

whereas in another city that would not be considered a quality case.

In neither case is it a Mom and Pop operation, but it is a different type operation.

MR. HODSON: Do you have occasion in the course of your review—since you have had wiretap authority—have you had occasion to deny an application for a tap simply because you didn't consider the case important enough?

MR. CLEVELAND: Absolutely, both at the beginning of the program and still today. They are always reviewed from a quality standpoint and are sometimes turned down because of that.

MR. HODSON: In other words, they meet minimum standards but you still turn them down?

MR. CLEVELAND: Still turn them down, yes, sir.

MR. HODSON: I was wondering now, turning to the report of the Administrative Office of the United States Courts—it indicates that you started out slowly in wiretapping in the Federal system and moved up to a high of 825 in 1971. From there you gradually decreased to this year or last year when you had 121.

Can you explain why this trend upward and trend downward? And is any of it the result of quality control?

MR. CLEVELAND: Yes, there are a couple of things involved here. One, the high level in 1971 was because of an emphasis being placed by the Strike Forces on gambling cases. And as a result there was a high number of Title III's throughout the nation.

Since that time, however, it has gone strictly on a quality concept, and depending on how the Strike Force feels about those particular cases.

And there again it depends on the area. Some Strike Forces contend that you have to have one of two criteria present before they will authorize prosecution in connection with the gambling case. In other areas, they are not so strict on that concept. Both are quality cases, but depending on the area you have a circumstance where they will prosecute or they won't prosecute.

MR. HODSON: Do you find that the quality of cases forwarded to you by the Strike Forces is better than the quality of cases generated by the United States Attorney's office?

MR. CLEVELAND: No, sir, I don't think I could say that.

MR. STAFFELD: I think they are two different areas, first of all. As we indicated before, the Strike Forces are in the major metropolitan areas where there is a high degree of organized crime and as a consequence have sophisticated gambling operations.

But that isn't to say that some areas where the United States Attorney is the prosecuting authority—that they aren't coming up with some quality cases as well.

MR. HODSON: Thank you.

PROFESSOR REMINGTON: I might just add one question that relates to the last question.

For a Commission such as this that is interested in Title III and its effectiveness and fairness, should it be concerned with what we understand is an issue and that is whether the Strike Force should continue?

MR. CLEVELAND: Insofar as the FBI is concerned, we are not members of any Strike Force. We do maintain close liaison with all of the Strike Forces, and I believe that the Department of Justice would probably confirm that we contribute a substantial amount to all of the work of all of the Strike Forces. It depends on the individual concept now as to whether a Strike Force is the proper way to approach the problem or not, and there is no agreement on that even within the Department of Justice.

PROFESSOR REMINGTON: Would it be a fair interpretation of what you have just said to conclude that you believe that Title III can work effectively with or without the Strike Forces?

MR. CLEVELAND: Title III would work effectively with or without the Strike Forces. The advantage of the Strike Force in connection with Title III's is the fact that they have the manpower and the know-how to handle Title III's. And from that standpoint it is very valuable.

Now, if you transfer that Strike Force under the United States Attorney there would still be the manpower and the know-how.

Hence the difference of opinion within the Department of Justice.

PROFESSOR BLAKEY: Are you saying, Mr. Cleveland, that unless you have access to the manpower and know-how of the legal people, Title III won't work?

MR. CLEVELAND: It would be very difficult if you didn't have that.

PROFESSOR BLAKEY: Do you have to have lawyer or prosecutor participation in the application of Title III's?

MR. CLEVELAND: Yes, sir.

PROFESSOR BLAKEY: One of the reasons Professor Remington and I were raising this is not with the Federal system in mind, but because you are always going to have United States Attorneys, but for the State people. What we are asking is do you think enacting the statute is enough to make it workable and worthwhile? I take it they are going to have to have special training for their police peo-

ple and their prosecutor people and they will have to make their prosecutor people and their police people sit down together. And that old-fashioned concept that the policeman does all the investigation and ties it up in a little knot and hands it over to the prosecutor who prosecutes by himself and they never talk except during trial will never work with Title III.

MR. CLEVELAND: It will never with only half of the things existing. You can have a Strike Force that is asked to conduct all manner of investigations and the investigations will be conducted. But unless they have the knowledge and know-how to sit down with that information and prepare papers and take it to court, it would all be fruitless.

MR. HODSON: I would like to ask just one more question. It has been suggested to me, at least, that the reason for the decline in the number of wiretap applications is because you are discovering that they are not as valuable as you thought they would be.

Would you comment on that?

MR. CLEVELAND: I would deny that insofar as our experience in the FBI is concerned. I can tell you very frankly that the decline in the use of Title III's in many instances in the FBI has been purely and simply because of lack of manpower to carry out the job.

When you lose a few hundred agents from your total commitment and all offices are down in the number of agents at the present time, you are not going to have that many Title III's because the manpower is not there to handle them.

They are manpower killers, no question.

MR. STAFFELD: Let me kill another thought on that line of the allegation that because it is easier to go through the State and not through the Attorney General that the Federal agencies are making use of State facilities in their State Title III's. In our case this is not true.

PROFESSOR BLAKEY: It is not true of the FBI but apparently it is true with the drug people.

MR. STAFFELD: I can only speak for FBI.

MR. KELLY: One other thing that contributes to this somewhat is that we have a tremendous backlog of cases, many of them involving Title III, which are in various stages of prosecution, and they haven't been finally adjudicated. And I think this has put strains on the Strike Forces and there is a limit to how much they can do.

PROFESSOR BLAKEY: I take it an investigative agent follows the case all the way through.

MR. KELLY: Yes, sir.

PROFESSOR BLAKEY: So if he works up three or four Title III's, eventually he is going to have to get in court on them, and when he is in court he is not on the street?

MR. KELLY: That is correct.

PROFESSOR BLAKEY: So, in effect, am I right in understanding that the success of the earlier Title III's, unless additional manpower is given to you, means that your agent power shifts now from investigation to trial?

MR. STAFFELD: Prosecution.

PROFESSOR BLAKEY: If you put in ten effective taps, then the following year you couldn't put in ten effective taps unless they gave you more people. So unless you get additional manpower your agents are all in trial?

MR. CLEVELAND: That is correct.

MR. STAFFELD: I think we are leveling off somewhat because in 1971 when we had that unfortunate overwhelming effort, it didn't let anything even out. And we are still suffering from it. We've got something like 2,500 subjects pending trial. And until we get that backlog out of the way we never will become on an even keel, so to speak.

PROFESSOR REMINGTON: Just one final question.

With regard to, say, research and—

PROFESSOR BLAKEY: The third final question?

[Laughter.]

PROFESSOR REMINGTON: The third final question. This is the last final question.

With regard to training Federal officers or State officers what is the role of the National Academy in this area? Has that been determined?

MR. CLEVELAND: The National Academy, formed in 1935, had as its purpose the training of executive police officers throughout the United States, and throughout the world, actually, so that they in turn could go back to their own departments and train their personnel and the over-all result would be a higher level of training of police throughout the country.

We think it has been very effective.

PROFESSOR REMINGTON: Is it likely to assume responsibility for the training of local law enforcement in the use of local Title III authority?

MR. STAFFELD: They have recently established a national organization of laboratory technicians which, I think, has been underway less than six months. And this is to face up to all problems of laboratory work, forensic sciences, electronics, and what have you.

I do not know specifically that they have undertaken training on assisting electronic surveillance work, but I am sure that this being a big part of laboratory work, it is going to be faced up to at sometime in the future.

PROFESSOR REMINGTON: Do you think that is a question that might be appropriately addressed to the staff of the Academy?

MR. STAFFELD: Yes.

MR. KELLY: I know as the Academy is presently constituted they receive at least four or five hours instructions on organized crime in general.

PROFESSOR REMINGTON: Okay.

Well, on behalf of the Commission and the Chairman who regrettably had to leave early, I

want to express the appreciation of all of us for your willingness to be with us today. We have found it most helpful and we thank you very much.

MR. CLEVELAND: Thank you, sir.

[Whereupon, at 4:25 p.m., the meeting was adjourned, to reconvene at 9:30 a.m., Wednesday, May 21, 1975.]

Hearing, Wednesday, May 21, 1975

Washington, D.C.

The hearing was reconvened at 9:35 a.m., in Room 3302, Dirksen Building, William H. Erickson, Chairman, presiding. Commission members present: William H. Erickson, Chairman; Richard R. Andersen, G. Robert Blakey, Samuel R. Pierce, Jr., Frank J. Remington, Florence P. Shientag, Alan F. Westin.

Staff present: Kenneth J. Hodson, Esq., Executive Director; David Cook, Esq.

PROCEEDINGS

CHAIRMAN ERICKSON: Good morning, ladies and gentlemen.

This morning we are privileged to have witnesses that will add to the Commission's work, and particularly we have the testimony of Edward Joyce, who is substituting for William S. Lynch, the Chief of the Organized Crime and Racketeering Section of the Department of Justice, who suffered some injuries on a weekend exercising tour that prevent him from being with us this morning. And Ed Joyce has graciously agreed to take his place.

Ed Joyce is the Deputy Chief of the Organized Crime and Racketeering Section of the Department of Justice and, as I understand it, he has served in that capacity for as many years as William Lynch. I think you have been there the same number of years, have you not, Mr. Joyce?

MR. JOYCE: About the same.

CHAIRMAN ERICKSON: And he is one of the nation's experts in this area.

We'd be very delighted if we could have Mr. Lynch, but we know of his problems and the injuries he suffered. We are equally delighted that you would give us the benefit of your expertise.

Will you be sworn, Mr. Joyce?

[Mr. Joyce was sworn by Chairman Erickson.]

CHAIRMAN ERICKSON: Thank you very much, Mr. Joyce. Mr. Cook will follow the procedure of our Commission of initiating the examination.

**TESTIMONY OF EDWARD T. JOYCE,
DEPUTY CHIEF, ORGANIZED CRIME
AND RACKETEERING SECTION,
CRIMINAL DIVISION, U.S.
DEPARTMENT OF JUSTICE,**

ACCOMPANIED BY ARTHUR PORCELLA, DEPUTY ATTORNEY-IN- CHARGE, SPECIAL OPERATIONS UNIT.

MR. COOK: Mr. Joyce, it is nice to have you here. I understand you do have a prepared statement, and you may proceed from that and augment it as you wish at this time.

CHAIRMAN ERICKSON: Do you have copies of that prepared statement?

MR. JOYCE: I do not. It was just retyped last night when I was informed I was coming up instead of Mr. Lynch, but I can supply this to the stenographer when we have finished.

CHAIRMAN ERICKSON: Wonderful.

MR. JOYCE: I want to thank the Commission for their kind invitation for me to appear and testify today.

As some of you may know, I have spent over 27 years in the Federal Government, 16 of that in the law enforcement field. I worked on organized crime cases as a departmental attorney from 1961 through 1969, and I have been working as a supervisor of such investigations and litigation since 1969 as a Deputy Chief of the Organized Crime Section. I have with me Arthur Porcella, the Deputy Attorney-in-Charge of the Special Operations Unit.

The Organized Crime and Racketeering Section operates in the field through 17 Strike Forces. Sixteen are assigned to specific geographic areas, and one is based in Washington which investigates and prosecutes cases involving racketeer infiltration of legitimate business.

A strike force is made up of an attorney-in-charge and five other departmental attorneys. Attached to this group of attorneys are representatives of each of the major federal investigative agencies who, under the direction and control of their parent agency, carry out the vast majority of the intelligence collecting and investigative activities of the group. The attorney complement contributes somewhat to this information-gathering process, but has only two avenues through which to make this contribution: the investigative grand jury and their participation in obtaining electronic surveillance orders pursuant to Title III procedures. From the pool of information collectively created

and shared come the basic facts finally acted upon in the organized crime cases which we prosecute.

A Title III investigation is always initiated by these field personnel. They digest a factual situation encountered and, if they believe electronic surveillance is appropriate, draw up a working application, supporting affidavit, and proposed court order. These are then sent on to the Special Operations Unit, which is the administrative unit charged with reviewing all such applications.

This unit is part of the Organized Crime and Racketeering Section and is under the supervision of an attorney equal in rank to the attorneys-in-charge of the strike forces. He has had experience on three different strike forces and acted as the attorney-in-charge of two of them. His deputy has had vast experience with Title III application papers and has served in this unit virtually since its inception. The remaining reviewing attorneys in this unit are, for the most part, recently recruited honor graduates who will eventually be assigned as additional or replacement personnel to the various strike forces. The number of such attorneys varies, but currently there are six such reviewing attorneys.

Upon their entry into duty, these attorneys are trained briefly on what to look for in a good set of Title III supporting documents. They are then assigned to doing the legal analysis and applying the taught parameters to the Title III applications received from the field. It is usual for them to find some difficulties with these applications, and they work with the attorneys and agents in the field in correcting such deficiencies as are found. In doing so, they are closely supervised by the Attorney-in-Charge of the unit and his deputy.

At the same time, a review of the same applications is usually in progress in the submitting investigative agency. Changes may also be made there, but the Special Operations Unit has the final say as to what goes into the papers that finally reach the desk of the Attorney General. When the investigating agency is satisfied with these papers, it sends them to the Department by covering memorandum to the Attorney General.

It is this memorandum that triggers the final formal processing of the applications. A final, complete review is done by the Special Operations Unit attorney assigned to the case. His recommendation of approval is reviewed by the Attorney-in-Charge or his assistant. His recommendation of approval is reviewed by the Deputy Chief of the Organized Crime Section who supervises the activities of the geographic area involved. His recommendation of approval is reviewed by a Deputy Assistant Attorney General who gives his recommendations to the Assistant Attorney General, Criminal Division.

Whether or not the Assistant Attorney General conducts a separate review is pretty much a matter of the desires of that particular individual. Assistant Attorney General Will Wilson did not review them, relying entirely upon the recommendations of his deputies. Assistant Attorney General Henry Petersen, I understand, made a general practice of independently reviewing each such application which crossed his desk.

At any rate, approval by the Assistant Attorney General causes the application to be forwarded to the Office of the Attorney General. There it is reviewed by the Assistant to the Attorney General and the Attorney General himself. If he approves, a letter of authority is sent to the strike force attorney or Assistant United States Attorney in the field.

While the review process I have described involved a strike force initiated application, the same route would be followed by those initiated by the United States Attorneys. Likewise, those drug case applications which are initiated by the United States attorneys and reviewed by the Narcotics and Dangerous Drugs Section, rather than the Special Operations Unit, follow the same route.

At any point along the way, the sufficiency of the probable cause or the propriety of using electronic surveillance in the situation described can be questioned by any reviewing official. An adverse determination on either of these points will cause rejection of the application.

While what I have described may seem cumbersome, we have found it workable. Once the file is complete with application, order and affidavit, the Special Operations Unit has found it can complete the initial review in two-and-one-half to three working days. The upper-echelon review which follows receipt of the request from the head of the concerned agency usually occupies another similar period of time. Overall, we have found that we can process these applications within five working days following completion of the file by field personnel. Since most organized crime cases involve continuing conspiracies, this time span is not generally a problem to us.

Because the warrant procedures for using electronic surveillance came into existence at about the same time the strike forces were deployed in the field, they have always been a part of the strike force effort. I have no way of comparing what a strike force would produce in the way of convictions without electronic surveillance with their present production. I think that the fact that over 80 per cent of the Title III applications approved in fiscal 1974 were obtained by strike forces indicates their relative importance to our work. And the Commission should bear in mind that few, if any, of

these cases would ever have been indicted through the use of conventional investigative techniques.

As I have said, our newly recruited attorneys quite literally cut their teeth on Title III investigative techniques. In addition, starting in fiscal 1974, they were given a formal course in supervision of Title III investigations in the field.

As a result of this experience and training, they are probably as well equipped to enter into Title III investigations as any group of attorneys or investigators in the country. Their use of the authority has roughly paralleled our overall prosecutive experience. That is to say, there have been a great number of Title III gambling investigations because the strike forces work more gambling cases than any other single category of offense. Areas in which assembling the necessary probable cause is difficult, such as in the area of major thefts which have already occurred, lead to a depression in that area of our figures on Title III usage. But Title III has always been of great advantage in situations in which a tightly knit, unchanging organization carries on a continuing offense in a set location.

In recent years, we have made some inroads into the infiltration or operation of legitimate business by racketeers in violation of 18 U.S.C. 1963, the so-called RICO statute. In the current fiscal year, almost 10 per cent of our Title III interceptions have been RICO-related.

But, apart from substantive cases, warranted electronic surveillance has proved of significant value in the intelligence field. It goes without saying that our agents and attorneys are not from racketeering backgrounds. Title III experience, however, gives them an understanding of the racketeer's vernacular and infrastructure which proves invaluable to them in later, ordinary investigation. In addition, warranted electronic surveillance gives the participating agency a highly accurate reading on the reliability of their informants.

In addition, as I have said, the attorneys' significant participation in the Title III process allows them to participate more fully in the investigative work of the strike force. This, in turn, understandably leads to a better attorney-investigator relationship. It is our experience that such a relationship has contributed markedly to the overall success of the strike forces. For most investigative agencies participate in joint investigations willingly only if they can derive from that relationship something they could not obtain on their own. If they find that they are the only ones making a contribution, they quite rightly wonder why they are participating in the joint effort. Title III and investigative grand jury work form the attorneys' contribution to the group's intelligence pool.

We have tried—and in my judgment succeeded—in using warranted electronic surveillance in a responsible manner. We wish to keep it that way. For this reason, we cannot point to any vast or innovative programs involving its use. Since we believe responsible use demands strict review of all applications by responsive public authorities, we would oppose any move to dilute that review or delegate it to lower authorities.

As you know, we have not had an uncluttered path in the use of Title III. To be specific, the controversies over our authorization procedures, minimization and—lately—those who should or should not be named in the warrant have cost us cases and convictions. But overall, the warrant procedure has allowed us to make cases in areas where cases had not been made previously. In Los Angeles, for instance, a Title III investigation enabled the FBI to arrest, and us to convict, a ring which 10 previous years of conventional investigation by the FBI had failed to bring to book.

In sum, I really don't know what we would have done without Title III authority.

As to the Commission's last interest, I believe the Criminal Division has previously supplied you with our views on consensual interceptions. They are extremely effective in bribery, extortion, and corruption cases. About one-half of the requests received by the Division are premised on an emergency situation. Placing these cases under a Title III-type warrant and approval system would, in my judgment, deprive us of their use in about 50 per cent of the situations in which we now find them helpful.

A consensual is usually undertaken in response to an opportunity to record evidence of a particular conversation which will never occur again. In this respect, they differ markedly from the usual Title III electronic surveillance. Such recordings have been approved by the United States Supreme Court, and I see no reason to bring them under the present Title III system.

That completes my prepared statement, Mr. Chairman. I'd be happy to answer any questions.

CHAIRMAN ERICKSON: Thank you very much.

Mr. Cook.

MR. COOK: Thank you, Mr. Joyce.

It is true, is it not, that the Federal Bureau of Investigation does not have a formal representative as such on strike forces?

MR. JOYCE: No, that is true on two of our strike forces, but in the large majority of the strike forces they do have a formal representative based at the strike force. This is a change from what occurred in the past, but that is the situation now.

MR. COOK: To what extent does the Federal Bureau of Investigation contribute to strike force investigations? Can you give any estimate of the proportion of strike force investigations which are aimed at offenses over which the FBI has jurisdiction.

MR. JOYCE: I would say it is probably in the nature of 85 to 90 per cent of the work of the strike force that is generated by the FBI.

MR. COOK: And some of the narcotics investigations, I think you indicated, are handled even in Title III situations by the United States Attorney's office?

MR. JOYCE: That is correct. Unless they involve hard-core organized crime, the drug cases are handled by the U.S. Attorney's office.

MR. COOK: How do you assure that a narcotics operation involving what you term a hard-core organized crime figure is brought to your attention?

MR. JOYCE: Well, under the guidelines that cover the jurisdiction between U.S. Attorneys and strike forces, the investigative agency is required to bring it in the first instance, if it involves organized crime, to the strike force. In the event that they do not bring the investigation to the strike force, then the United States Attorneys are required to refer it to the strike force. And in the normal give and take on a strike force, the agent will usually know what is going on in his district, and he usually brings it to the strike force's attention, at which time the strike force—if the U.S. Attorney has not brought it over—will go to the U.S. Attorney's office and ask for it. If there is any question as to who has jurisdiction, it is referred back to the Department for a decision.

MR. COOK: I think you indicated that some narcotics Title III's ostensibly not involving hard-core organized crime figures are reviewed by the Narcotics and Dangerous Drug Section.

MR. JOYCE: That is correct.

MR. COOK: What division or section is this unit a part of?

MR. COOK: That is a section in the Criminal Division. It is a separate section. The Narcotics and Dangerous Drugs Section is headed by Mr. William Ryan.

MR. COOK: And under Mr. Ryan, are there attorneys who review the applications?

MR. JOYCE: That is correct.

MR. COOK: Similar to the Special Operations Unit?

MR. JOYCE: That is correct.

MR. COOK: Do these applications for Title III's ever come through the Organized Crime Section after review by the Narcotics and Dangerous Drugs Unit?

MR. JOYCE: Yes. We get copies of all their applications. The original application goes from the section to the Deputy Assistant Attorney General.

MR. COOK: But in terms of the actual approval of the request and implementation of the investigation in the field, I take it there are some narcotics investigations that are carried on completely independently of the Organized Crime Section.

MR. JOYCE: That is correct.

MR. COOK: Do you follow up on these cases in terms of liaison or keep track of what they do?

MR. JOYCE: No, not particularly. There just haven't been that many. The procedure is there for it to happen, but there haven't been very many going through from DEA to the Drug Section without our approval.

MR. COOK: At any rate, it is the purpose and intent of the Organized Crime Section to insure that any prosecutions of major or significant organized crime figures are handled by the statute?

MR. JOYCE: That is correct; that is correct.

MR. COOK: Would it be your judgment that the training that is acquired by the attorneys who are newly joined and assigned to the Special Operations Unit, and then, I take it, farmed out to strike forces, acquire a special expertise in the handling of Title III's?

MR. JOYCE: Oh, yes. They get special training, as I have said. But they get the actual operational experience of working with the people in the field to put the Title III into its proper form. And when they go to the field, they are pretty well experienced in what is a highly technical and precise legal operation.

MR. COOK: Do you have any idea of the percentage of strike force attorneys, and particularly those who handle Title III's, who have come up through the Special Operations Unit as opposed to those attorneys who might join the strike force from a U.S. Attorney's office in that same district?

MR. JOYCE: Well, of the younger attorneys, the attorneys that we have hired since we have used the Title III's, I'd say it's about 95 per cent of the attorneys going out to the strike forces have gone through that Special Operations Unit.

MR. COOK: Do you have any idea of approximately how long the typical recruit or new attorney will stay with the strike force or section?

MR. JOYCE: Well, so far we have been very lucky. We have had very little turnover among our younger attorneys. We have had more turnover with our senior attorneys where they gain a reputation in the community and are offered much more than we can pay them. But our younger attorneys—we have been lucky to keep almost all the good ones.

MR. COOK: Do you have any idea of the average length of time that the assistant United States attorney remains with that office after joining it?

MR. JOYCE: No. That always depends on the area of the country, and it depends upon the politics, that is, which administration is in power. In some areas when there is a change of administration, there is a change of the entire office. In some other areas, the larger offices like Los Angeles, Chicago, and New York, there is carry-over from one administration to another.

But that is the exception rather than the rule.

MR. COOK: A change of administration, in any event, does not affect personnel on the strike forces; is that correct?

MR. JOYCE: That is correct.

MR. COOK: Is it fair as a general statement to say that the average strike force attorney remains with the Justice Department longer than the average assistant United States attorney. Do you have any basis on which to make that kind of judgment?

MR. JOYCE: Yes, that is my judgment. I may be what you call biased with respect to that, but my judgment is that we keep our attorneys longer than the U.S. Attorney does. And I think the proof of that is that most of our strike force chiefs have come up through the ranks of our strike forces. Very few of them come in from the outside.

MR. COOK: So the section has a considerable investment in terms of the expertise which is obtained by newly hired attorneys that remain with the section and, as you say, in some cases go on to become strike force chiefs.

MR. JOYCE: Oh, yes, and I think that is reflected in the fact that we handle most of the Title III applications, because we do have that experience. And many of the United States Attorneys realize they don't have it and ask us to handle Title III's for them.

MR. COOK: Based upon your experience, would you say that it would be damaging to the present quality of Title III investigations if this authority were transferred from the strike forces to the Office of the United States Attorney.

MR. JOYCE: I would say it would be very damaging. Again, I have a particular viewpoint because of my position, but as I perceive it, the expertise in the field could be wiped out at the end of an administration if it was transferred to the United States Attorney's office.

MR. COOK: So in a very real sense you feel, at any rate, there is an identity of interest between the implementation of Title III and the strike force concept.

MR. JOYCE: Yes.

MR. COOK: You stated that the first-line reviewers are generally honor graduates—the newly hired people?

MR. JOYCE: That is correct.

MR. COOK: We have heard testimony during this set of hearings that it is an obstacle in some sense and slows down the reviewing process to the extent that it is necessary to educate these newly acquired personnel in Title III procedures which are submitted by people who have had experience with Title III's in the field. Let me ask you if you agree with that assessment?

MR. JOYCE: Yes. The only way we can train the young attorneys is by putting them in to do the work, and it does somewhat slow down the review.

However, the senior people in the unit are very capable and we are able to move the Title III's and perform the training, which on balance is what we should be doing, I think.

MR. COOK: So the trade-off in terms of lost time versus experience gained is necessary and desirable from your viewpoint?

MR. JOYCE: Yes.

MR. COOK: Staying with the length of the review process—and I think you have made clear that it is your belief that this is justified and necessary—we have had testimony from the personnel in the Headquarters Section of the Federal Bureau of Investigation that their review process seemingly involving a comparable number of layers, if you will, takes place in a much shorter time. I think they said it was less than two to three days on the whole.

Has the section made any efforts to cut down its own reviewing time so, in effect, the affidavit is not waiting on the Organized Crime Section judgment before implementation?

MR. JOYCE: Yes, we did. We now require logging of the time periods: when the affidavit first comes in from the field; when it is first sent forward by the attorney; when it is passed on to the Deputy Chief; and when it is passed on to the Deputy Assistant Attorney General. And by keeping that log and setting a five-day limit, five working days, on the unit, we have, in fact, speeded up the process. And while the senior official from the FBI may be correct, I think in most cases the application on the affidavit comes over before we have finished our review. There are many occasions when the application has to wait before going to the Attorney General, and it has to wait on the memorandum from the investigative agency.

MR. COOK: That raises an interesting question.

At a previous set of hearings, the Commission heard testimony from a strike force chief that he did not think the Federal Bureau of Investigation or any other investigative agency had a proper func-

tion in making a legal judgment on the sufficiency of proper cause in the affidavits and applications.

Do you think that they perform a needed function, or do you think that this is something that you would more or less accommodate them with for their own happiness or satisfaction?

MR. JOYCE: I think it performs a needed function. They always exercise some kind of a judgment with respect to proper cause—on search warrants, on arrests. Because they make the judgment first that there is probable cause for arrest before they apply for the warrant. I don't see why they should not have their own supervision and discipline applied to their applications and affidavits for a Title III.

MR. COOK: The Organized Crime Section, I believe, based on our studies in the field, is currently implementing Title 18, United States Code, Section 1964, I believe, by the imposition of civil remedies?

MR. JOYCE: That is correct.

MR. COOK: It seems to me I recall a law school maxim that you cannot enjoin a crime, but apparently this is no longer true under the Federal Code. Could you give the Commission some idea of the advantages and ways in which the Section is using this statute in its operations?

MR. JOYCE: Well, the one case, the *Cavetto* case in Chicago, where we utilized it, was a gambling case. It was based upon a Title III, and it didn't show the great amount of volume of gambling, nor did it have important organized crime people in it, and we knew from past experience that if we tried the case it would take a long time to try, and we probably would get probation from the judge at the end of it.

So rather than go through the criminal process, we drew up a temporary restraining order and a preliminary injunction and served it on all of the defendants, enjoining them from conducting their gambling operation.

After the preliminary injunction was granted, we then served notices for the taking of depositions of all of the people concerned, and we called them in. We had already applied for the right to make an application to the court to compel their testimony under the so-called immunity statute.

They came in and they refused to testify in the deposition, and we took them before the court, and the court ordered them to, saying that they would be immune from use of their testimony against them if they did testify.

They again refused, and they were all incarcerated on civil contempt and they are still in the Cook County jail, I believe.

MR. COOK: How long will they be incarcerated?

MR. JOYCE: A maximum of 18 months.

MR. COOK: Or until they purge themselves of contempt?

MR. JOYCE: Until they purge themselves?

CHAIRMAN ERICKSON: This was based on the grand jury.

MR. JOYCE: This was not a grand jury. This was a deposition. And the immunity statute provides that even in a grand jury that has a three-year-life, the maximum sentence can only be 18 months.

MR. COOK: Do you contemplate the use of this apparently effective section in other areas?

MR. JOYCE: Yes, we do. As a matter of fact, we are very delighted with the Seventh Circuit opinion in *Cavetto* and distributed it to all our strike force chiefs for use in the appropriate situation.

MR. COOK: Can you briefly summarize the issues that were raised by the defendants in their appeal to the Seventh Circuit in that case?

MR. JOYCE: Well, as I recall, they said that they could not be compelled to testify; that the immunity statute didn't apply to a civil proceeding; that they couldn't, in a civil proceeding, be forced to incriminate themselves.

And maybe Mr. Porcella knows more about the issues raised.

MR. COOK: I take it the deposition proceeding is substantially identical to the civil deposition proceeding with representation by counsel?

MR. JOYCE: That is correct.

MR. COOK: You also mentioned that you had had some appellate problems with the naming of persons in a Title III warrant, the need to name all the persons against whom you had probable cause, or if you left some out you left yourself open to some kind of judgment of acquittal or suppression.

Can you describe for the Commission the issue that was raised in this case?

MR. JOYCE: Yes. The statute requires the naming of the people to be overheard, and where in the one situation a man's wife, Minnie Kahn, was not named in the warrant, the District Court suppressed the evidence against her husband because we had not complied with the requirement of the statute to name all the people we had reason to believe would be overheard. And they felt that since the wife—the telephone was at the residence—that we had reason to believe the wife would be overheard. And it was suppressed, but it was reversed.

MR. COOK: Does the District Court in this situation conduct an evidentiary hearing and make an ex post facto judgment upon whom the investigative agency should have had probable cause?

MR. JOYCE: Yes. Invariably in a Title III, we have evidentiary hearings.

MR. COOK: I take it this poses a fairly hard judgment for you to make, or at least for the agents

to make, on insertion of names in the warrant. On the one hand, you would be required to have sufficient probable cause against anybody you named, at the risk of putting in a name against whom you do not have sufficient probable cause.

MR. JOYCE: That is true. And what happened in the *Kahn* situation—we knew that she would be overheard, but we didn't know she would be overheard in gambling conversations. But she was overheard in gambling conversations, and the court, looking at it, said we should have included her name.

MR. COOK: Mr. Chairman, that concludes the staff's questions.

Thank you very much.

CHAIRMAN ERICKSON: Thank you, Mr. Cook.

Mr. Porcella, I judge that you may be answering some of these questions that I may propound to Mr. Joyce. In accordance with the rules of our Commission, would you be sworn as well?

[Mr. Porcella was sworn by Chairman Erickson.]

CHAIRMAN ERICKSON: I might ask a few preliminary questions.

I am certain you have seen the report on applications for orders authorizing or approving interception of wire or oral communications relating particularly to the period from January 1, 1974, to December 31, 1974, prepared by the Administrative Office of the United States Courts.

MR. JOYCE: I haven't seen that, no. Mr. Porcella has it, as a matter of fact, in front of him.

CHAIRMAN ERICKSON: Well, I was reviewing that, and on Table 7, on page XVI, it points out the intercept applications which were authorized. Do you have that before you?

MR. PORCELLA: Is that Arabic or Roman numeral XVI?

CHAIRMAN ERICKSON: Roman number XVI.

MR. JOYCE: Yes, we have it in front of us.

CHAIRMAN ERICKSON: I notice as we look at that particular chart that in 1968 the intercept applications which were authorized was 174, and that all of those were state applications; that none were applied for in the Federal courts. And, of course, that is understandable in view of the passage of the Act.

Going on to 1969, there were 301 applications, 268 of which were state and 33 of which were Federal. And I note that of the applications authorized, only 30 were installed. Some 33 were authorized, but only 30 were installed on the Federal level.

Would you have any idea as to why they weren't installed after they were authorized?

MR. JOYCE: Yes. As happens very often in gambling cases, the more sophisticated gambler will

move and change his telephone number and move his office. And if these were microphone installations, it was probably because they moved their office. If they were telephone installations, it was probably because they changed their number between the time that we got the probable cause and the installation was to be made. That happens quite frequently.

CHAIRMAN ERICKSON: Now, would you be able to estimate what percentage of these Federal applications were for the purpose of surveilling gambling operations?

MR. JOYCE: In 1969, the 30?

CHAIRMAN ERICKSON: Yes.

MR. JOYCE: Probably around two-thirds.

The first one we had dealt with counterfeiting, and then we had some good, hard drug cases in the beginning.

CHAIRMAN ERICKSON: In 1970 the number increased to 182, and you actually installed 179. The state level of applications authorized rose from 268 to 414, according to the report in 1970.

And the question I would have would be: As we see this increase—and according to the report, it hit its high in 1971 for the Federal applications at 285—could you explain how these figures fall in this range or category, the increase from, say, 33 to 182 and from 182 to 285?

MR. JOYCE: Well, in 1971 we started what we called Operation Anvil and what the Bureau calls the intensification program, where we asked the Bureau to go out and put in as many gambling Title III's as they could during the football season in order to get a firm analysis of what the gambling magnitude was in the country.

And that intensification program peaked in 1972, and they were mostly the gambling cases.

CHAIRMAN ERICKSON: When did Operation Anvil start?

MR. JOYCE: It started in the football season of 1971—September '71 through the end of the season in March or April of '72.

CHAIRMAN ERICKSON: And can you tell us what this Operation Anvil was?

MR. JOYCE: Well, just the intensification of the gambling investigations utilizing Title III's. We required that the Bureau—and Mr. Mitchell required from Mr. Hoover that the Bureau install the Title III's, but serve no search warrants until the Title III was analyzed, until the transcripts were prepared, and serve no arrest warrants until the time the indictment was returned.

And it was just to get some kind of a figure as to how much gambling was going on in the United States.

The only figure I had ever seen before was one that I was instrumental in establishing, and that was in 1961 when we had wiretaps from New York State. And the only way we could get any kind of a national figure was to take the population of the area covered by the New York State Investigation Commission, the amount of gambling conducted there as shown by the wiretaps, and multiply it by the proper multiple to extract it for the United States.

CHAIRMAN ERICKSON: So the purpose was to find the scope of national gambling?

MR. JOYCE: Yes. Everybody was gambling. Everybody was speculating as to how much gambling there was going on in the United States, and nobody knew. But this would give us a hard-core figure for that football season.

And it turned out that of 100 operations that were investigated during that Operation Anvil, they had a gross handle of \$1.5 billion. And we estimated that we probably only got about anywhere from 2 to 5 per cent of the action in the United States in those 100 operations. And if you use that multiplier, you have something on the order of anywhere between \$35 billion or \$60 billion a year in the hands of gamblers.

CHAIRMAN ERICKSON: As you know, many of the critics of Title III have claimed that these Title III intercepts have been used to impede small gambling operations at great expense to the government and without really making any penetration into organized crime or any real change in the law enforcement picture.

I think you have probably seen some of the materials that have been written in that regard.

MR. JOYCE: Yes.

CHAIRMAN ERICKSON: What would be your answer to that?

MR. JOYCE: Well, my answer is that we have penetrated organized crime activities. Our analysis of Anvil—now, this was done by going over all of the tapes and reviewing all of the conversations that were taken on Title III.

Our estimate is that 43 per cent of those operations were, in fact, run by or owned by hard-core organized crime personnel; and that practically all the operations had some kind of dealings with organized crime. That is, they were either getting line information through organized crime channels or laying off to organized crime people.

And we haven't had another Operation Anvil which we will have to do sometime soon so we can find out what the volume of gambling is today, as opposed to what it was in '71 and '72.

CHAIRMAN ERICKSON: In your opinion was the operation a success?

MR. JOYCE: Oh, an unqualified success, because now for the first time we have had a hard sampling of the gambling activity in the country, and we could make our estimates based upon that firm sampling, which we never had before.

CHAIRMAN ERICKSON: In your opinion, did the results of this make any inroads into organized crime?

MR. JOYCE: Oh, yes. It made inroads insofar as it forced the moves. When we first started in Operation Anvil, we could see that there was some little activity in Las Vegas, but that most of the activity was around the country. And our informant information and all the other hard information we get now shows that most of the lay-off in the United States goes into Las Vegas.

So we have had the effect of making a move—of the main lay-off bookmakers making a move from the local areas into Las Vegas.

CHAIRMAN ERICKSON: Did any prosecutions come about by reason of these taps?

MR. JOYCE: Oh, yes. I think there were 250 convictions obtained in the hundred operations that we penetrated.

CHAIRMAN ERICKSON: What percentage of these prosecutions would have been of major organized crime figures as contrasted to the local bookmaker or the person that has a small gambling operation?

MR. JOYCE: Well, we didn't go into any real small gambling operations, although some of them have been characterized that way, as "Mom and Pop" operations. One particularly in Oklahoma was characterized as a "Mom and Pop" operation. He and his wife were handling it, but the man was one of the major bookmakers in the U.S.

CHAIRMAN ERICKSON: This "Mom and Pop" operation, as denominated, was not in your opinion properly designated in that way?

MR. JOYCE: It certainly was not. There aren't very many "Mom and Pop" gambling operations, because, first of all, a bookmaker in order to make a living has to have a high volume of bets. The average sports bookmaker works on a percentage of 4.5 per cent profit, and you can see that in order to even keep a "Mom and Pop" going, you have to have a private high volume business. And in order to maintain your operation for harassment by law enforcement officers, in order to pay for the services that you need, that is, in order to pay off and get the late line information, you have a large overhead that has to be paid from this small margin of profit.

CHAIRMAN ERICKSON: Without benefit of legislation of the type set forth in Title III, would it have been possible to determine what the scope of national gambling operations was?

MR. JOYCE: No, it would not. We have tried in the past, but without the Title III you don't get the hard information.

You may, in one bookmaking operation, recover the week's records with a search warrant. In another operation you may recover, say, two months. In another operation, you may not recover anything.

The only way you can get and retain the actual volume of betting conducted by a bookmaker is through an intercept, either a microphone installation or a telephone.

CHAIRMAN ERICKSON: Well, prior to the time that Title III was passed, the Department of Justice, the Federal Bureau of Investigation, was operating under the proscriptions of the Federal Communications Act, particularly Section 605 thereof, which was interpreted to mean intercepting and not divulging.

So prior to this you could have, using your Department interpretation, intercepted as many calls, but the only prohibition would have been against using that information in evidence.

Isn't that correct?

MR. JOYCE: Well, that was the feeling of some, but nobody in the Department ever suggested that we tap the bookies. As a matter of fact, even where the IRS was only using pen registers, we lost in the court, and the evidence was suppressed.

And we have been pressing for wiretap legislation ever since 1961.

CHAIRMAN ERICKSON: The point I am trying to make is: There was the interception of conversations under the interpretation of Section 605 before that time, so this did occur and it did occur in the Las Vegas area, did it not?

MR. JOYCE: I know of no wiretaps conducted by the Federal investigative agencies in the Las Vegas area prior to the enactment of Title III. You are probably talking about the installation of microphones.

CHAIRMAN ERICKSON: Well, there were installations of microphones.

MR. JOYCE: That is the only illegal surveillance—so-called illegal surveillance—that was conducted by the Federal investigators. I personally feel that that was one of the greatest counterespionage operations against organized crime ever conducted.

CHAIRMAN ERICKSON: That was the effort to ascertain the skimming operations that were going on at Las Vegas?

MR. JOYCE: That is correct.

CHAIRMAN ERICKSON: Now, in connection with that investigation, there were these bugs installed. And the reason that they were installed is

that it was impossible to determine what the skim was.

MR. JOYCE: What the skim or the activities, the other activities of the people who were considered to be organized crime targets.

CHAIRMAN ERICKSON: And there was some information that would indicate there was some concert of action between the various hotels.

MR. JOYCE: Oh, yes.

CHAIRMAN ERICKSON: To the effect that the skim would even be a particular percentage on a particular night.

MR. JOYCE: Yes.

CHAIRMAN ERICKSON: And that was relayed to the various hotels through a particular public telephone; is that not correct?

MR. JOYCE: That may very well be. I am not aware of all the details.

CHAIRMAN ERICKSON: But without the use of these intercepts, even though they were characterized as illegal, it would have been impossible to determine the extent of this conspiracy.

MR. JOYCE: That is correct.

CHAIRMAN ERICKSON: Or the skim?

MR. JOYCE: Yes.

CHAIRMAN ERICKSON: And at least there has been an inference from time to time that that might have been organized crime.

Was that such an operation in your mind?

MR. JOYCE: Oh, no question.

CHAIRMAN ERICKSON: And there was some indication they were acting in concert?

MR. JOYCE: No question in my mind about that either. That has been confirmed by Title III's.

CHAIRMAN ERICKSON: Was it large? Was the operation such that it involved more than one hotel or more than one casino?

MR. JOYCE: Yes, it involved a number of them, and it still does, as a matter of fact.

CHAIRMAN ERICKSON: What is skimming?

MR. JOYCE: Skimming is the taking from the casino the money that is earned in the gambling operation prior to accounting for the winnings in a taxable form. It is taking non-taxed money out of the casinos.

In the early '60's, they'd take it right out of the count house. That is, when they'd take the drop box which contains all of the cash used at the table back into the count house to count it, the owners would stuff the money in their pockets and walk out.

CHAIRMAN ERICKSON: Was that referred to as "black money?"

MR. JOYCE: It may well have been.

In one of the cases that Mr. Loewy handled, there was over a million dollars a year coming out of one casino.

The way they did it was they had 11 tables, and they had three shifts, so they would take out \$100 per shift per table when they were counting, which comes to \$3300 a day, \$100,000 a month, \$1.2 million a year. And that was being taken down to Miami every month.

All it takes is two chips off the table to mount up to that vast amount of money.

CHAIRMAN ERICKSON: And the surveillance activity that was involved was the installing of microphones or bugs in certain of the casinos?

MR. JOYCE: That is correct.

CHAIRMAN ERICKSON: And there was a recording made of everything that occurred in particular—

MR. JOYCE: I am not sure that it was always recorded.

CHAIRMAN ERICKSON: During particular hours?

MR. JOYCE: It was listened to.

CHAIRMAN ERICKSON: It was listened to and some of it was recorded, and recordings were done at the FBI Headquarters there in Las Vegas?

MR. JOYCE: Yes. I am not sure now it was at the FBI Headquarters.

CHAIRMAN ERICKSON: I think it was under the name of Wilbur Clark and Associates, Inc.

MR. WESTIN: Mr. Chairman, I think there was a leased premise called the Henderson Novelty Company.

MR. BLAKEY: But the address was the FBI office.

MR. JOYCE: I don't know why I am answering the questions. You seem to know more about it than I do.

[Laughter.]

CHAIRMAN ERICKSON: The material at that time, even if this was an illegal bug—as long as it was intercepted, but not divulged—did not constitute a violation of Section 605?

MR. JOYCE: Section 605 did not apply, because it was not a telephone.

CHAIRMAN ERICKSON: Right.

And so as far as being in violation of any law, at that time it did not violate any law?

MR. JOYCE: Well, it violated the Fourth Amendment.

CHAIRMAN ERICKSON: Oh, yes, but apart from the one opinion of the Supreme Court of the United States suggesting that there might be a civil remedy for violation of the Fourth Amendment, there was no violation of any criminal statute, such as now would exist if you operated in violation of the provisions of Title III.

MR. JOYCE: Well, some of the installations were made through a technical trespass.

CHAIRMAN ERICKSON: Right.

MR. JOYCE: And without an authorization to make such a trespass, inherent as it is in Title III, there was probably a violation of some state statutes.

CHAIRMAN ERICKSON: Yes, I am aware of that. But there was no Federal violation. If there was a violation it was of state statute or state law.

MR. JOYCE: That is correct.

CHAIRMAN ERICKSON: The reason for that is to point out that now that we have Title III there are more protections against any illegal surveillance accorded than there were prior to the enactment of Title III.

MR. JOYCE: Well, that is correct, except for the period from '65 on where all of the so-called illegals were terminated—from '65 to the enactment of Title III.

But now, the rights of the people who might be surveilled are much more closely protected than they were before.

CHAIRMAN ERICKSON: Because you have these series of procedures that must be followed?

MR. JOYCE: Yes.

CHAIRMAN ERICKSON: Now, one of the other points that goes directly into this is the fact that as the procedures existed prior to the enactment of Title III, the electronic surveillance techniques that were available to investigating authorities changed from Attorney General to Attorney General, and in different Department interpretations; isn't that correct?

MR. JOYCE: Well, if you are talking about the intelligence, the security taps, that probably did change from Attorney General to Attorney General. But aside from those taps, which we have always considered to have been legal, I don't know of any Attorney General—

CHAIRMAN ERICKSON: Well, each Attorney General took a position. Ramsey Clark took one position on wiretapping and electronic surveillance.

MR. JOYCE: He took it on Title III, as a matter of fact.

CHAIRMAN ERICKSON: Yes, but prior to that, other Attorneys General took positions as well.

MR. JOYCE: Well, under Attorney General Kennedy we were pressing for wiretap legislation. We wanted the authority to do it. I don't know of any Attorney General who ever authorized any wiretaps other than in the internal security field.

CHAIRMAN ERICKSON: And in the internal security field, each one did express different opinions, or they changed from time to time with different Attorneys General.

MR. JOYCE: I am not aware of that. I have no awareness of what their feelings were with respect to internal security wiretaps.

CHAIRMAN ERICKSON: Well, going on to this chart, if I may, without belaboring this, we hit the high on the taps in 1971 with the 285 taps.

In 1972, the state went up again to 649, but the Federal intercepts were reduced to 206—or the authorized intercepts. Could you explain that?

MR. JOYCE: Well, I don't know why the state rose, but ours went down because it was winding down.

CHAIRMAN ERICKSON: On Operation Anvil?

MR. JOYCE: Operation Anvil—the concentration on the gambling operations, gambling intercepts.

CHAIRMAN ERICKSON: Now, in the period 1971-1972, what percentage of those would have been gambling intercepts or authorized intercepts?

MR. JOYCE: Just giving a guess, I'd say about 75 per cent of them were for gambling.

CHAIRMAN ERICKSON: What type of crime would be involved in the other intercepts?

MR. JOYCE: Loansharking, drugs, counterfeiting, fencing.

CHAIRMAN ERICKSON: Is there any connection between organized crime and loansharking?

MR. JOYCE: Oh, very much so; very much so.

CHAIRMAN ERICKSON: Is that tied into gambling?

MR. JOYCE: Very often it is a direct result of the gambling losses.

CHAIRMAN ERICKSON: In 1973, the reduction went down all the way to 130. Is there an explanation for that?

MR. JOYCE: Well, I think there was a “wait and see” attitude on the part of the investigative agencies, to see what was going to happen with our court problems with respect to the authorizations in the *Giordano* and *Chavez* cases.

And as you know, there was a lot going on during that period of time.

CHAIRMAN ERICKSON: Has Watergate had any influence?

MR. JOYCE: I think it has probably influenced the entire government in some fashion or other.

CHAIRMAN ERICKSON: In 1974 there were only 121. And this ties into the same picture.

MR. JOYCE: That is right.

CHAIRMAN ERICKSON: The reason for these questions is to ask if Title III was ineffective and if that was one of the reasons that there was a reduction.

MR. JOYCE: Oh, no. Nothing could be further from the truth. Title III was extremely effective. It has been effective in all of the investigations that we have used it in. It is an invaluable tool. I don't think we could do as much as we have done in the organized crime field without it.

CHAIRMAN ERICKSON: Have conviction percentages gone up in those cases where Title III intercepts have been received in evidence?

MR. JOYCE: Oh, yes. As a matter of fact, in pleas, too. We just had a recent case in California where the boss, the underboss, a capper, and two members pleaded guilty to a violation of 18 U.S.C. 1962, because of the installation of a microphone—and also turned an informant. But the informant was turned also because of the installation of the microphone.

CHAIRMAN ERICKSON: For the purpose of the record, what is Title 18 U.S.C. 1962?

MR. JOYCE: That is the infiltration of legitimate business. It is called the RICO statute, which I think is very appropriate for an organized crime acronym.

CHAIRMAN ERICKSON: The technical name for RICO is the Racketeer Influence on Corrupt Organizations Act?

MR. JOYCE: That is correct.

CHAIRMAN ERICKSON: In your experience with the use of this statute, do juries react favorably to the receipt of this evidence, or are they adverse? Do they turn it down just because of the fact that it's a private conversation which was being intercepted? Or do they generally receive it?

MR. JOYCE: I don't have any first-hand knowledge. I have never tried a Title III case myself. But I haven't heard anybody complaining that the jury was turned off, particularly when the agent is a clean-cut FBI agent who explains the installation, and then they start playing the tapes and, as usually happens, the defendants start being cowed by their own voices coming over.

CHAIRMAN ERICKSON: One of the defense lawyers that testified before suggested that the juries love it, that they receive it, and convictions are nearly a certainty. Is that an overcharacterization?

MR. JOYCE: No, I can't recall having lost any good cases where we have had Title III's, except where we lost them on pretrial motions. As a matter of fact, probably one of the best Title III investigations we ever had was really Mr. Cook's in Detroit, where they had the *Anchor Bar* Case. It was suppressed because of the authorization problem.

CHAIRMAN ERICKSON: In your opinion, the strike force concept is definitely tied into Title III?

MR. JOYCE: Oh, yes, I think they go hand in hand; they were just made for each other.

CHAIRMAN ERICKSON: It would be a major error to change the strike force concept?

MR. JOYCE: I think it would be a major error to change the strike force concept without Title III in any event, but this adds more weight to the argu-

ment for keeping the strike force, that is, that the strike force is so appropriate a vehicle for the installation and the conduct of Title III investigations.

CHAIRMAN ERICKSON: Now, from your experience in dealing with organized crime—and I judge from what you have said that there is a tie-in between organized crime and gamblers—would it be possible to adequately surveil any of these operations without the benefit of the Title III provisions?

MR. JOYCE: It can be done, but not as well. It could be done by infiltrating the gambling. It could be done by getting the probable cause and watching the telephone toll records and making raids. But it is on a hit-or-miss basis. It is not as certain as the Title III installation is of getting the proof of the crime.

CHAIRMAN ERICKSON: Even if you went that route, would it be possible to determine the exact extent of what did occur in the commission of the crime?

MR. JOYCE: No, it would not. It would be very difficult to prove the case, particularly in a 1955, to show a volume of at least \$2,000.

CHAIRMAN ERICKSON: What is 1955, for the record?

MR. JOYCE: That is the basic gambling statute that gives the FBI jurisdiction to investigate gambling without the necessity of having interstate operations.

CHAIRMAN ERICKSON: In dealing with these statutes, is the immunity statute tied in in any way to the use of Title III in combatting the crime problem?

MR. JOYCE: Oh, yes. As I explained, particularly in the *Cavetto* case, we probably, without the immunity statute, couldn't have forced those people to the deposition. They just would have taken Five.

CHAIRMAN ERICKSON: In your experience, have there been occasions from time to time when a simplified procedure would have been of value to you in obtaining wiretap information?

MR. JOYCE: Yes, there have been occasions. And in some of those occasions, the strike force attorney went to the state and asked the state to install them because they could do it quicker.

But in the vast majority of the situations, a more streamlined, but less carefully reviewed procedure, I think, would be counterproductive.

CHAIRMAN ERICKSON: Has your office ever used the emergency provisions?

MR. JOYCE: No.

CHAIRMAN ERICKSON: Is there a reason for that?

MR. JOYCE: The Attorney General has refused to authorize them. Each Attorney General has refused to authorize anybody to conduct the emergencies.

CHAIRMAN ERICKSON: Has any application ever been made for permission to use the emergency?

MR. JOYCE: No, the guidelines have just been established that they will not be.

CHAIRMAN ERICKSON: Do you feel that which we would portray as a cumbersome procedure, with the many steps that have caused some of your men to go to the state level to get more prompt action, are necessary at the Federal level?

MR. JOYCE: Yes.

CHAIRMAN ERICKSON: And you don't quarrel with that? You don't think any simplifications or improvements could be made in the statute?

MR. JOYCE: No, I think the review we make is a responsible review, and I think it ought to continue.

CHAIRMAN ERICKSON: Just a few other questions on consensual taps.

Those are essential, are they not?

MR. JOYCE: Pardon?

CHAIRMAN ERICKSON: Consensual taps, if you will, or the use of a body wire on a person for the purpose of determining what the actual conversation is—do you feel that is an invasion of privacy?

MR. JOYCE: Well, if it is, I don't feel it is an unreasonable invasion of privacy. It is usually used in order to catch somebody who is going to inculcate himself in the commission of an offense. And I think really all it is is for the courtroom. Because the man who wears the body microphone can always testify with respect to the substantive conversation. But he may be impeachable; he may have a record; he may just not be a credible witness.

CHAIRMAN ERICKSON: And it is putting it in concrete so it can't be changed.

MR. JOYCE: Yes.

CHAIRMAN ERICKSON: And that is of value?

MR. JOYCE: It is of very great value, being able to corroborate a witness who may be part of the original crime.

CHAIRMAN ERICKSON: Has this been necessary on occasion even for protection purposes of law enforcement persons?

MR. JOYCE: Yes; yes, particularly where the agent or the informer is going into a room by himself with these people that he is dealing with. It is important for the surveillers to know what is happening in that room.

CHAIRMAN ERICKSON: I am deeply indebted to you for your testimony, Mr. Joyce. I will now turn the questioning over to other members of the Commission.

Professor Blakey.

MR. BLAKEY: Could I clarify a couple of points, Mr. Joyce. You indicated young honor graduates go into the Special Prosecution Units?

MR. JOYCE: That is right.

MR. BLAKEY: Are honor graduates still being hired in the Organized Crime Section?

MR. JOYCE: Yes.

MR. BLAKEY: Without prior experience?

MR. JOYCE: Yes.

MR. BLAKEY: It had been my understanding a recommendation was made as a result of the strike force study that there be some experience criteria applied to people being hired in the Organized Crime Section.

MR. JOYCE: Well, that's fine if you get the applicants. And when we do get people with Federal criminal experience, we do hire them for the strike force program.

But we have a necessary input into our program. We have 162 attorneys. And we have some of them leaving almost every day. And we have to hire. So the only place where we can get them is either from the honor graduates or from the JAG Corps. And that is where we procure most of our attorneys.

MR. BLAKEY: So I understand that the recommendation is really now a preference for experienced people?

MR. JOYCE: Yes. We will take them if we get the applications.

MR. BLAKEY: You testified earlier that most of the lay-off business has moved from other areas in the country into Las Vegas?

MR. JOYCE: That is correct.

MR. BLAKEY: Is the lay-off business in Las Vegas legal or illegal?

MR. JOYCE: Both.

MR. BLAKEY: Would you explain what you mean?

MR. JOYCE: Well, it is not a violation of Nevada law for a legal bookmaker to take lay-off bets as long as he pays the Nevada tax. But there are a lot of them who are not paying the Nevada tax.

MR. BLAKEY: How are the communications relayed from say, Chicago, to Las Vegas?

MR. JOYCE: Many times pay phone to pay phone.

MR. BLAKEY: Wouldn't that relay from Chicago to Las Vegas be a violation of Title 18 U.S.C 1084?

MR. JOYCE: Oh, yes, they are violations of 1084.

MR. BLAKEY: So the lay-off business being conducted in Las Vegas is, insofar as it involves interstate communications, illegal?

MR. JOYCE: Yes. It is probably a violation of both 1952 and 1084. That is, it's a violation of the gambling statute—

MR. BLAKEY: Would you explain how the business being operated in Las Vegas is legal?

MR. JOYCE: It is legal under state law, even though it violates federal law. That is the distinction.

MR. BLAKEY: There was some confusion on that point.

At the time the microphone surveillance was being conducted from the late 1950's through July of '65, was there, during that period of time, some discussion within the Department as to the legality of the microphone surveillance? Am I correct that there were instructions given from the Attorney General to the FBI that some of that microphone surveillance was lawful?

MR. JOYCE: I am not aware of that.

MR. BLAKEY: Maybe I should back up and ask you this question: Are you familiar with the course of communications that took place between the Attorney General and the FBI from the period, say, 1955 through July of 1965, discussing the legality of wiretapping and the legality of microphone surveillance in the areas of domestic surveillance, international surveillance, and organized crime, insofar as it would fall within either of those two categories?

MR. JOYCE: No, I am not very aware of it.

MR. BLAKEY: So if we really wanted to pursue the perceptions both in the Bureau and the Department itself as to whether it is lawful or unlawful, we would need another witness.

MR. JOYCE: You certainly would. As a matter of fact, I think you'd probably be the best.

[Laughter.]

MR. BLAKEY: Mr. Joyce, you indicated that you have been in the Organized Crime and Racketeering Section, actively involved in prosecution and aware of the general intelligence picture available to the Federal Government since about 1961. Obviously, I can't ask you to quantify, but would you give us your best estimate, professional judgment, as to whether the organized crime program of the Federal Government has had an impact, turning the corner, or no impact at all, on the organized crime situation?

MR. JOYCE: I think it's had a severe impact on the organized crime picture, particularly on the hierarchy.

In Chicago, there is just nobody around who apparently is willing to take over running the business.

MR. BLAKEY: How about in New England?

MR. JOYCE: New England, the same way. Until Patriarca got out of prison just recently, they were in complete disarray.

MR. BLAKEY: What is the situation in New York?

MR. JOYCE: Well, the Columbo family is in pretty bad shape, and we haven't had as hard an impact in the New York area as we have had elsewhere, mainly because the problem is so much greater in New York than it is any other place.

MR. BLAKEY: What about in New Jersey?

MR. JOYCE: We have had a severe impact on the DeCalvacante family.

MR. BLAKEY: DeCalvacante was convicted as a result of a wiretap; is that correct?

MR. JOYCE: That is right.

MR. BLAKEY: Could you give us an estimation of what happened to his family in its other, non-gambling, activities as a result of his indictment and conviction?

MR. JOYCE: No.

MR. BLAKEY: The question I am asking is: Do gambling prosecutions against organized crime leaders—and I am speaking about the LCN—have an impact on their non-gambling activities?

MR. JOYCE: They necessarily have an impact. That is, if the leader is engaged in either trial or is incarcerated, it slows down the activities—all the other activities. If the gambling money isn't forthcoming, then it is hard to bankroll his family, it is hard to pay for the protection he needs in order to conduct his operations, it is hard to pay his overhead for the other activities such as narcotics.

MR. BLAKEY: Wouldn't he have money available from narcotics or fencing to bankroll his activities?

MR. JOYCE: He may have some, but he really needs the bankroll from the gambling in order to buy the narcotics.

MR. BLAKEY: I thought narcotics was a very lucrative activity?

MR. JOYCE: It is.

MR. BLAKEY: Isn't there enough money generated in narcotics to finance itself?

MR. JOYCE: That is not our perception, no. That is, it may be able to finance the narcotics purchase initially, but the ongoing expenses of paying each of the members, paying the police—

MR. BLAKEY: If narcotics doesn't pay for itself, why do they do it?

MR. JOYCE: It is not self-supporting. That is my point.

MR. BLAKEY: If it is not self-supporting, why are they in it?

MR. JOYCE: Because it does add income and it does help carry.

MR. BLAKEY: If it adds income, then it is not only self-supporting, it is more than self-supporting. You don't get income from something that has cost in excess of its income. Am I right?

MR. JOYCE: We are talking about two separate points. I am saying that the narcotics—organized crime narcotics—is not sufficient to accumulate the money needed to purchase the narcotics, and also to pay the money to the members, the salary that they are paid and to pay for all the other overhead that the organized crime would have.

MR. BLAKEY: You mean overhead in non-narcotics areas?

MR. JOYCE: That is right.

MR. BLAKEY: You have testified, Mr. Joyce, that you were in the program both before Title III and after Title III, both before strike force and after strike force.

Am I correct that there were attorneys in the field acting in a quasi-strike force capacity before they were formally established?

MR. JOYCE: Oh, yes, yes, there were.

MR. BLAKEY: Could you make a relative judgment of how effective those attorneys were in the field operating without the wiretap authority as compared to how effective they are now with it?

You have seen some of the same people—not different in the way they get up in the morning and the way they go to work—operate against the same kind of investigative problem, once with wiretap and once without. In which situation are they more effective?

MR. JOYCE: I think it's clear that we are more effective with the wiretap than we were beforehand. We weren't completely ineffective.

MR. BLAKEY: Attorney General Ramsey Clark has testified that his organized crime program without wiretapping was just as effective as it might be. Would you agree with that opinion?

MR. JOYCE: Oh, no. I would not.

MR. BLAKEY: Were you a member of his organized crime program?

MR. JOYCE: I certainly was. We are seeing the effect every day of the installation of microphones under Title III and installation of telephone taps, particularly on the hierarchy of organized crime, and back before the use of the wiretaps there was a lot of talk about the insulation of the bosses; that they are completely insulated, you'd never be able to penetrate them; that they don't get involved in the operations. And we are learning that it is just not true. We are hearing the Zerillis and the Columbos, and we are seeing their intricate involvement in the gambling and narcotic investigation.

MR. BLAKEY: During the period of around July of 1965, are you familiar with the study that was conducted by Cary Parker in the Criminal Division of a series of illegal surveillances?

MR. JOYCE: I heard that—no, I am not familiar with the details of the study.

MR. BLAKEY: Attorney General Ramsey Clark in July of 1973 testified before the Justice and Legal Affairs Standing Committee of the Canadian House of Commons—and I am quoting from his statement at that time, Issue No. 21, page 10:

“The idea that wiretapping is effective against organized crime is (material omitted) wrong-headed in my judgment. (material omitted.)

“I had an examination made of 12 bugs that had been installed on alleged members of organized crime. They were in place an average of nearly two years each, and grown men, professional police, supposedly agents of the FBI, sat 24 hours a day, seven days a week, 365 or 366 days a year, waiting for someone to say something that they should not say.”

Attorney General Clark left the Canadian Parliament committee with the impression that that illegal surveillance that was conducted in the period between the late 1960's and the middle of 1970's simply got nothing.

Are you familiar with the product of that surveillance?

MR. JOYCE: I am familiar with the product of some of the surveillance, yes. And if we could have used the evidence obtained on those so-called illegals, we could have decimated organized crime, particularly in Chicago.

MR. BLAKEY: In your professional judgment, is Clark's estimation of those illegals correct?

MR. JOYCE: No, it is not correct. And I can't imagine any better evidence to use in a conspiracy involving organized crime people than their very own words, particularly when they have a feeling of safety and they are being candid with each other.

MR. BLAKEY: Mr. Clark also testified before the Canadian House of Parliament, Issue No. 21, page 15—and he is having reference now to the Mitchell problem, and he says that the prosecutions apparently lost because of the Mitchell issue “could have gone forward without the wiretapping. They did not need it but they had it in there and they messed up good cases.”

In your judgment, could any of the reported 600 cases that may be lost because of the Mitchell issue have been made without wiretapping?

MR. JOYCE: Some of them could have been and so we are making them, that is, where we had enough evidence to go against some of the people. But certainly—

MR. BLAKEY: So some of those cases are being saved?

MR. JOYCE: That is right.

MR. BLAKEY: As to some of the people?

MR. JOYCE: As to some of the people.

MR. BLAKEY: But not all of the people?

MR. JOYCE: Oh, no. We have lost a great deal through that *Giordano* problem, and they could not have been made otherwise.

MR. BLAKEY: And it is your testimony as to some of the cases, that nothing is being saved?

MR. JOYCE: On the vast majority, nothing is being saved.

MR. BLAKEY: Would you agree with Attorney General Clark's judgment that you could have done all that without wiretapping anyway?

MR. JOYCE: No. And the best example is that *Anchor Bar* case where 18 police officers were indicted because of the installation of the television camera and the microphones. We couldn't have indicted any of them on the evidence that we had, absent the wiretap.

MR. BLAKEY: When Mr. Clark was Attorney General, did the Organized Crime Section communicate with him as to what was going on and what was happening?

MR. JOYCE: Oh, yes. He got daily reports, as our procedure, on everything that was occurring.

MR. BLAKEY: Did you see those daily reports?

MR. JOYCE: I saw the ones that—during that time my assigned area was Ohio, and I saw all of the ones that dealt with Ohio, yes.

MR. BLAKEY: Were you generally familiar with what was in the other reports?

MR. JOYCE: Oh, yes.

MR. BLAKEY: Was there anything in the reports provided by the section to Mr. Clark that could have led him to make these public judgments as to the ineffectiveness of wiretapping?

MR. JOYCE: No. I can't imagine anybody in a responsible position in the Organized Crime Section saying that.

MR. BLAKEY: I obviously cannot ask you what Ramsey Clark thought. But I can certainly ask you as to what communications came up from the Organized Crime Section of which you were aware that could have led him to reach this judgment.

In short, the question I am asking you is: Is there anything the Organized Crime Section gave to him that could have justified this public position that he took then and is taking now?

MR. JOYCE: No, the general feeling in the Section was that he was wrong.

MR. BLAKEY: I have no further questions.

CHAIRMAN ERICKSON: I think we'd better take a break at this time.

We'll take a five-minute recess.

[Whereupon, a short recess was taken.]

CHAIRMAN ERICKSON: May we proceed.

Judge Shientag is going to be forced to leave. I will be willing to waive our order—

MS. SHIENTAG: No, not at all. I am not forced to leave. I will wait my turn.

CHAIRMAN ERICKSON: Professor Westin.

MR. WESTIN: Mr. Joyce, you testified, if I understood you correctly, that about 75 per cent of the Title III interceptions the Chairman was asking you about from the list dealt with gambling cases; is that correct?

MR. JOYCE: That is my gut reaction.

MR. WESTIN: You also testified that based on the information learned from these Title III interceptions, you estimated somewhere between, as I heard it, \$35 billion and \$60 billion was being handled by organized crime nationally, as you extrapolated from the Title III wiretaps, a year; is that correct?

MR. JOYCE: That is correct.

MR. WESTIN: Who is doing this gambling? Who provides the \$30 billion and \$65 billion that is being handled?

MR. JOYCE: It depends on what type of gambling it is. A lot of the numbers activity comes from the ghetto areas in the major cities.

I guess there is almost a complete cross-section of the United States with respect to who is gambling.

MR. WESTIN: Have you ever tried to develop a figure as to how many Americans are gambling, ranging all the way from numbers to the middle-class and upper-class gambling on football pools? Have you ever tried to figure out what percentage of the American public is committing crimes daily in gambling?

MR. JOYCE: Well, I am not sure that the gambler commits a crime when he gambles the way the professional does when he accepts the wagers. In most states it is not a crime to make a bet; it is a crime to be in the business of accepting bets.

MR. WESTIN: Let me try to change my question: Have you tried to make an estimate of how many Americans are involved in placing wagers?

MR. JOYCE: No, we are not doing it, but I understand that is one of the projects of the Gambling Commission.

MR. WESTIN: If I said 50 million Americans, would that be in the ballpark?

MR. JOYCE: Fifty million?

MR. WESTIN: Different individuals. I am not talking about repetitive bettors. I am trying to get at how many Americans are engaged in the activity you are investigating.

MR. JOYCE: It is very difficult to say. We could probably get the number of people who are engaged in the gambling operations that we surveil, but it is difficult to establish a multiple, that is, what percentage of the actual gambling is going on we are, in fact, covering.

MR. WESTIN: Well, if I take some kind of lower-to-upper figure such as you did, \$35 billion to \$60 billion, which is a pretty big spread for us to apply to people who do our budgets—

MR. JOYCE: If you can supply us what \$1.5 billion on a \$100 operation—if you can tell me what the multiple is, you can get the figure.

MR. WESTIN: So if we are dealing in tens of billions, would you think 10 million or 20 million Americans betting would be a minimum, at least?

MR. JOYCE: Oh, I'd say a minimum. I'd say maybe as much as a fourth to a third of the people in the United States bet at some time during the year on a football game or numbers or dice game.

MR. WESTIN: One of the things this Commission is trying to look at is whether the activity engaged in of wiretapping and bugging are being directed at the right place.

I wonder if you'd comment on some difference we have had in testimony as to whether you actually stop much of this gambling activity, looking at it either from the end of the number of people placing the bets, or the organized crime organization that is conducting it.

Trying to make my question specific, you have testified that in several places—New England, Chicago—you had impeded substantially the hierarchy of organized crime through Title III intercepts. Yet, the picture we have gotten fairly frequently is this may take place temporarily—it may impede it for a matter of months before reorganization takes place, a year or something like that, but with a quarter to a third of the American population deeply interested in continuing their betting activities the organization restructures itself, regroups and so forth, and new organizations come forward.

And when you have a picture of an activity which seems to be so deeply built into the structure of American society and the wishes of its population, what are you really accomplishing by the type of activity that puts somebody in jail for a time and slows it up. What, over a longer period, a three-year look or five-year look, is the result on the activity if you spend so many millions or tens of billions in fighting organized crime, but it goes on without substantial change?

MR. JOYCE: We have never claimed that we are destroying organized crime. I think a better analogy would be to a cancer that is stable. It is not metastasizing as it would without treatment, but it is not in remission, either.

That is, the organized crime picture and the illegal gambling would be much more widespread that it is now if it weren't for our actions.

And a good way to assess that is to look at the picture in the United States before we started our organized crime drive and then look at it now.

Before we started our organized crime drive, there were illegal casinos down at Homestead in near-by Virginia an up and down the panhandle of West Virginia. They were practically all around the country. They were at Saratoga. They were down in Miami, in Biloxi. They are no longer there.

In each of those casinos, incidentally, that we raided—and I am talking about those that the FBI raided—in each of those casinos we found the games were rigged, that is, that the dice tables were rigged. They were using electrical cords and using dice with steel filings in them in order to control the games.

MR. WESTIN: That is good consumer protection activity on the part of the Bureau and Department of Justice, but did you just replace the gambling activity that was taking place in those illegal casinos with other types of betting activities? That is, the persons that would go there either bet now through the local apparatus or fly more often to Las Vegas.

MR. JOYCE: I think by our activity we have stimulated the junket business into Las Vegas, and Las Vegas is growing by leaps and bounds. The handle out there is just fantastic.

MR. WESTIN: If we think about the privacy issues and law enforcement effectiveness, how would you react to the suggestion that if either through legalization of gambling or through the consumer protection type activity that you have described, the recommendation from this Commission might be that the Federal law ought to deal more directly with the question of legalization of gambling rather than assuming we should continue wiretapping authorization for a pursuit of gambling activity—

MR. JOYCE: I have never heard of any feasible system of legalizing gambling. In the sports betting operation, as I explained, the margin of profit is 4.5 per cent. And I just can't imagine any governmental agency operating on that kind of a profit. I think that in the places where gambling has been legalized, it has proven that it is no sinecure for organized crime.

We find organized crime in Las Vegas. We find it in the gambling casinos. We find it in the bookmakers, where they are supposedly legal—to the same extent that it is anywhere else.

The off-track betting can't compete with the bookmaker. In all the taps we have had on in the New York area, we have never heard one bookie say, "The OTB is beating my brains out." All it is doing is stimulating more people that will eventually go to a bookie.

I have heard no feasible statement for the legalization of gambling. Even if the state could compete with the bookies in the sports betting operation, they wouldn't be able to lay it off. Who can a state lay off to? Another state?

And if they didn't lay off, then they'd take an awful risk of a beating, a bad beating.

As you probably know, in a game like the Bullets-Warriors game, there is a lot of sympathy in the San Francisco-Oakland area for Oakland, and there is a lot of sympathy in Baltimore and Washington for the Bullets.

Now, assume that Maryland is in the bookie business and they take all of that local action, everybody betting on the Bullets. If the Bullets lose, the State of Maryland would be taking a risk of losing millions upon millions of dollars unless it could lay off to a similarly situated betting operation in San Francisco where they would balance off the action on San Francisco against the action on Baltimore.

And if they don't do that—then there is also the other factor involved, and that is that the chances of the quarterback on the team, where the legal betting is going on, being subjected to bribes in order to beat the state. It would be very great.

MR. WESTIN: You mean the government gets into the business of bribing the quarterback?

MR. JOYCE: No, it would be the bookie who is betting into the government who would be bribing the quarterback.

MR. WESTIN: Your general answer is that you don't believe it is possible to set up a legalized substitute for the gambling system as it runs nationally today for the kind of reasons you have described?

MR. JOYCE: That is right. The only possible type of gambling operation that could be run would be a numbers operation.

MR. WESTIN: Some testimony we have had in the last couple of days raised the question of whether when you do your interceptions you are productive in getting leads to persons higher up, when you are using Title III's in the surveillance of gambling operations.

Has it been your experience, looking at the Title III's that you have had experience with that some, most, or few of these produce leads to higher-ups, as opposed to providing evidence for the particular individuals that you have identified already in probable cause warrant applications, and so on.

In general, what has your experience been in this?

MR. JOYCE: I'd say in the beginning of a gambling investigation, where we have probable cause for a bookie operation, the chances of getting up to the higher-ups are very good. That is, once we get

on the wires and find out where the other offices are, we can usually penetrate the entire operation.

MR. WESTIN: Could you supply us with substantiation of that? That is, if you went back and looked at your cases, would you be able to furnish us with examples that would indicate that? We had some testimony in which one particular FBI office, eight or nine Title III wiretaps were put on—

MR. BLAKEY: Excuse me, Alan. That was DEA.

MR. WESTIN: Was it? A DEA office—that the efforts to get higher-ups had not worked out in all but I think one of those cases.

Would you be able to give us examples where, having had probable cause for one level in a book-making operation, you had moved up and gotten presumably indictments; or just to clarify that, did you get intelligence information or information that led to indictment and prosecution?

MR. JOYCE: I am talking about leading to indictment and prosecution of higher-ups, yes.

MR. WESTIN: Would you be able to supply our Commission with that so we can have examples of actual cases that have gone to court?

MR. JOYCE: We'd have to do it with the closed cases.

MR. WESTIN: You have had a long enough period that you'd be able to supply us with some examples of that?

MR. JOYCE: Yes.

MR. WESTIN: You mentioned the *Minnie Kahn* case where the lower court suppressed the evidence on the grounds she had not been named in the warrant, and this was reversed on appeal.

MR. JOYCE: Right.

MR. WESTIN: Has that been a problem in general, that you have difficulty in naming all people who may make incriminating conversations in advance? Or is that a very exceptional situation?

MR. JOYCE: No, particularly in a gambling operation, in the very beginning you are usually working with informant information. And the informant may tell you that so and so is operating a gambling business at this point.

No, you have no way of knowing in the beginning how many of his associates are calling in.

MR. WESTIN: So you viewed the lower court opinion as being unreasonable in requiring that you give the names of all persons you might find making incriminating conversations?

MR. JOYCE: Yes.

MR. WESTIN: When the appellate court reversed that, did it do so on the ground that you had acted reasonably in those that you had named and that it was unreasonable to expect you to list the wife's name?

MR. JOYCE: That is substantially what it was.

MR. WESTIN: I'd like to ask you one other question. When you were describing the civil pursuit, and you mentioned that you were taking civil depositions and then using your immunity powers to require that individuals give testimony, and when they refused to use immunity they then would be indicted for contempt. Do you have a feeling as to whether that eliminates the requirement for a grand jury or other kinds of mechanism which American law has traditionally seen as the true form for the production of testimony in criminal proceedings? Doesn't that, in other words, give you the power, in bringing a civil proceeding, to require the giving of testimony in what traditionally has been criminal law context, with its grand jury system, with its court proceeding, et cetera?

Does it trouble you that we are washing out the grand jury?

MR. JOYCE: Oh, we are not washing out the grand jury at all. That is one case we used it in, and we used it because we didn't think it was worth the prosecution. All of these bookmakers could have come in and could have agreed to stay out of business. They could have testified. What we were looking for was to make them witnesses to testify against the higher-ups. But they, for their own reasons, refused to testify.

MR. WESTIN: I think what I am trying to get at is in a normal criminal proceeding you would have had to go before a grand jury, am I correct, in order to bring a criminal proceeding?

MR. JOYCE: That is correct.

MR. WESTIN: And here you are setting up an alternative procedure of bringing a civil procedure which goes on the filing of a complaint, I assume, or filing of a motion.

MR. JOYCE: It is not outside the judicial system. The judge can refuse the temporary restraining order. He could have refused the temporary injunction or the permanent injunction. At any point in time he could have refused us our remedy and it could have been reversed on appeal.

MR. WESTIN: So you are saying if this is to be policed, you are counting on the judiciary to do it, if they feel there is an impropriety in it or it is taking away constitutional safeguards. Your feeling is the court can limit you as to it?

MR. JOYCE: If you are speaking of abuses of the system, I am not counting on the judiciary, but on ourselves to prevent any abuses. That is the prosecutor's initial duty, and I think we can prevent any abuses.

If there is a step after the use of our discretion, then the court certainly has the power to stop us.

MR. WESTIN: Thank you, Mr. Chairman.

CHAIRMAN ERICKSON: Thank you.
Professor Remington.

MR. REMINGTON: Mr. Joyce, if I may, I'd like to pursue the question of judicial review for a moment.

In your experience, what has been the quality of the judicial review of applications under Title III?

MR. JOYCE: Well, it has been, I think, very detailed. The review has been very close. This is apparently a subject that raises a lot of emotional issues, and depending upon the courts we have had to explain, and have lost in the initial stages because we followed the formal procedures in all other business, that is, of having a subordinate sign an assistant attorney general's name to a letter. And I think the courts, in general, have been going over the applications and comparing them to the statutes, in some instances with great care and in great detail.

MR. REMINGTON: Is the judge's concern under Title III the same as or different from his concern under Rule 41, for example, in a case such as that which was described in Detroit, where I assume there was a Title III application, and another application under Rule 41 to put in a TV monitor?

MR. JOYCE: I think that their concern with the Title III procedures is much greater than the concern, so far as I have been able to see, with any other type of activity, investigative activity.

MR. REMINGTON: So that if one were to try to characterize judicial concern with the protection of Fourth Amendment interests, one would say that concern is greater when an application is made under Title III to conduct electronic surveillance than it has been on the whole when an application is made under Rule 41 to conduct a physical search.

MR. JOYCE: I would say the concern is much more evident in Title III.

MR. REMINGTON: And the protection, therefore, of the individual's interest, insofar as that is left to the judiciary, is greater under Title III than under Rule 41?

MR. JOYCE: Yes, sir.

MR. REMINGTON: Given that concern on the part of the judiciary for these cases, how do you explain the fact that when it gets to the sentencing stage, judges seem to feel often, particularly in the gambling area, that the matter is of very little importance, as reflected in the sentence—if that is a fair characterization.

MR. JOYCE: It is very, very spotty. I have tried a number of cases, gambling cases, where the sentences have been in excess of eight years. But in other areas, we are pretty sure that all we are going to get is probation. And it depends generally upon the area.

In some parts of the country you can count on heavy sentences for people involved in gambling.

As a matter of fact, there was just a sentence of a major gambler out in Hawaii yesterday for income tax evasion, where he was sentenced to 24 years for income tax evasion. And the income he was evading was from his gambling operations.

So it varies.

MR. REMINGTON: Is that difference primarily the difference in who the judge is, or is it the difference in the attitude of the communities in which the judge is sitting?

MR. JOYCE: I think most judges are products of the community where they are sitting and they tend to reflect the attitude.

MR. REMINGTON: Insofar as you know, has this issue been a subject of discussion, in the various institutes for judges, on sentencing, when they come together to talk about problems? Do they tend to confront this issue?

MR. JOYCE: The Department has attempted to raise it wherever it was appropriate at the meetings, yes.

MR. REMINGTON: I raise that question because I concluded from your testimony that in your view the success of the investigative effort is measured not in terms of the amount of gambling, but rather the impact on the organization. Is that a fair characterization of what you said earlier?

MR. JOYCE: Well, I don't think you can divorce them. I think the impact on the gambling, the illegal gambling, has an impact on the organization.

MR. REMINGTON: But the impact would be greater on the organization if the sentence were such as to take the person out of operation, is that true?

MR. JOYCE: That is true; that is true.

MR. REMINGTON: Is it that judges disagree with that or that they tend to see the matter in conventional sentencing terms, that is, how serious is the offense, whereas the investigative agency may be asking the question of how serious is this person's participation in the overall scheme.

MR. JOYCE: I just couldn't speculate upon what the motives of the judiciary are.

MR. REMINGTON: The reason I ask you is because I think if you look at the situation you see an investigative agency feeling that these cases are very important, and the need for adequate investigative authority, including Title III, is very important. You look at it from the other end and see other fair-minded and able people apparently reflecting the view that the cases are quite unimportant. And in attempting to answer the question of how important is Title III, it seems to me one has to somehow come to grips with what apparently is a quite different attitude about the significance of these cases between the investigative agency, on

the one hand, and the member of the judiciary on the other.

The question is: How should we resolve it?

MR. JOYCE: I think the investigative agency and the prosecutor are the only ones who have the best overall view of the impact or the roots of the gambling operation. I think those judges who are aware of those roots usually sentence fairly firmly. I think it is only the judges who are not convinced that there is a serious national problem with respect to the organized crime involvement in organized gambling that give probation.

MR. REMINGTON: Thank you.

CHAIRMAN ERICKSON: Judge Shientag.

MS. SHIENTAG: Thank you, Mr. Chairman.

Mr. Joyce, in the presentation of cases to the grand jury, your office has jurisdiction along with the U.S. Attorney's offices in various jurisdictions; is that right?

MR. JOYCE: That is right. We present our cases usually to the grand jury.

MS. SHIENTAG: And when you present Title III wiretap evidence to the grand jury, in what form is that presented?

MR. JOYCE: Well, if it is a voluminous gambling case, it is probably presented in summary testimony by the agent. If it is a serious extortion and there are some threats on the wires, we'd probably play the tape.

MS. SHIENTAG: When you play the tape, you have all the equipment in the grand jury room.

MR. JOYCE: That is correct.

MS. SHIENTAG: And what do you do about extraneous material? I am thinking of minimization.

MR. JOYCE: Well, if it is necessary to play the tape, we will play only that part of the tape that is pertinent. We wouldn't be playing the rest of the nonpertinent conversation. Very often, we make a second tape from the first tape with only the pertinent portions on it, and then play that.

MS. SHIENTAG: Is that second tape also sealed? Does it have a protection for purity of evidence that is required?

MR. JOYCE: No. When we play a tape in a grand jury, that is usually a duplicate of the original. The original is sealed until the time of the trial.

MS. SHIENTAG: So that very often before the grand jury you would present hearsay evidence or secondary evidence that wouldn't be appropriate at a trial?

MR. JOYCE: That may well be.

MS. SHIENTAG: Summaries, for example, by the agent wouldn't be the best evidence.

MR. JOYCE: That is right.

MS. SHIENTAG: Now, the defendant's attorneys have access to grand jury minutes, isn't that true?

MR. JOYCE: They usually have access to the testimony of a witness before the grand jury, the same as a *Jenks Act* statement.

MS. SHIENTAG: And have you ever had attacks on the evidence based on this sort of evidence?

MR. JOYCE: No, not since *Costello*. Since the Supreme Court said, "You can use hearsay evidence," we haven't had any successful attacks.

MS. SHIENTAG: I see. Just one more question.

Have you ever known of a case where using the grand jury, as opposed to other methods, you secured further evidence or probable cause that led you to make another application for Title III wiretaps or electronic surveillance?

MR. JOYCE: No, I am not aware of any situation. I used a grand jury one time, in 1966, to get probable cause for a search warrant. But I only did it once, and I have never heard of it being used to get probable cause for a wiretap.

MS. SHIENTAG: I want to thank you, sir, for your intelligent testimony.

CHAIRMAN ERICKSON: Chief Andersen.

MR. ANDERSEN: No questions.

MR. BLAKEY: Mr. Chairman, could I clarify two points?

CHAIRMAN ERICKSON: Professor Blakey.

MR. BLAKEY: Mr. Joyce, when you authorized the *Capetto* case to be brought, it was a civil proceeding, wasn't it?

MR. JOYCE: Yes.

MR. BLAKEY: It was not a criminal proceeding?

MR. JOYCE: Yes.

MR. BLAKEY: Was it possible to have a criminal fine as a result of that proceeding?

MR. JOYCE: For the contempt?

MR. BLAKEY: I am talking about the complaint itself. Did it look forward to a criminal fine?

MR. JOYCE: It looked forward to just restraining the activity of the gamblers.

MR. BLAKEY: Did it look forward to criminal imprisonment?

MR. JOYCE: No, it did not.

MR. BLAKEY: When the witnesses refused to respond to the deposition, you then had two options. You could have gone for criminal contempt or civil contempt.

MR. JOYCE: That is right.

MR. BLAKEY: If you had brought a criminal contempt and wanted more than six months imprisonment, would you have had to have a jury trial?

MR. JOYCE: Yes, when you have an indictment, then you have a jury trial.

MR. BLAKEY: When you go into a civil proceeding, is it possible to secure punitive imprisonment?

MR. JOYCE: No, it is to coerce—to force the witness to testify.

MR. BLAKEY: Are you familiar with the general processes that enforce the antitrust laws?

MR. JOYCE: No.

MR. BLAKEY: Does the Department have an option in antitrust areas to go criminally or civilly?

MR. JOYCE: I believe so.

MR. BLAKEY: Are you familiar with the procedures under the Food and Drug Act? Do they have an option there to go criminally or to go civilly?

MR. JOYCE: I'd just be speculating, Professor.

MR. BLAKEY: The reason I ask that is that it seemed the record ought to be left clear that there are a number of statutes, including the Wage and Hour Laws, that give the government the option to go civilly or criminally, and these are traditionally felt to be not inconsistent with civil liberties.

Thank you, Mr. Joyce.

CHAIRMAN ERICKSON: Mr. Joyce, you have been extremely helpful, and we again thank you for your testimony. I hope that the testimony—

MR. WESTIN: Mr. Chairman, Professor Blakey's comment prompts me to go to redirect. May I ask one more question?

MR. JOYCE: Recross?

[Laughter.]

MR. WESTIN: This exchange now and then.

Is it your opinion that the Department of Justice has never sought to use immunity in wage and hour or antitrust or the other kinds of procedures described by Professor Blakey to put people into coercive situations where they are put in prison for having declined to answer?

MR. JOYCE: If you are relating it to just a deposition, the answer is I have no information about it. But I do know that prior to the repeal of all of the immunity statutes, in the antitrust field you had an immunity statute—that is, anybody who testified became immune from prosecution, and that was the normal procedure in the way of conducting grand jury investigations. But I don't know if they ever used it in their civil investigations.

CHAIRMAN ERICKSON: It is also done in the securities and exchange field, is it not, civil or criminal?

MR. JOYCE: Yes.

CHAIRMAN ERICKSON: Thank you very much, Mr. Joyce.

And Mr. Porcella, we appreciate your assistance as well.

MR. JOYCE: Thank you very much, Mr. Chairman.

CHAIRMAN ERICKSON: Our next witness is Mr. Peter Schlam, Assistant United States Attorney, Brooklyn, New York.

Will you be sworn?

[Mr. Schlam was sworn by Chairman Erickson.]

TESTIMONY OF PETER SCHLAM, ASSISTANT UNITED STATES ATTORNEY, BROOKLYN, NEW YORK

CHAIRMAN ERICKSON: Mr. Cook.

MR. COOK: Thank you, Mr. Chairman.

Mr. Schlam, will you tell the Commission what your present position is?

MR. SCHLAM: Yes, sir. I am Assistant United States Attorney.

MR. COOK: And whereabouts?

MR. SCHLAM: In the Eastern District of New York, which is Brooklyn, New York.

MR. COOK: What are your principal duties at the present time?

MR. SCHLAM: My principal duties are as a prosecutor. I am specifically involved primarily now in international narcotics conspiracy cases.

MR. COOK: Do you as a matter of course or on occasion use the wiretapping statute in your investigations?

MR. SCHLAM: We have, sir, but to a limited extent.

MR. COOK: What other methods have you used in prosecuting these narcotics conspiracies?

MR. SCHLAM: Primarily we use what is known as accomplice testimony or co-conspirator testimony, which in summary form is the process where, based on testimony of a member of the conspiracy, we develop cases against his co-conspirators.

MR. COOK: What methods do you use to obtain this kind of testimony?

MR. SCHLAM: Well, basically the method used is the one of attempting to induce a person to cooperate with the United States Attorney by offering him a plea to a lesser count and bringing to the attention of the judge that will sentence him the fact that he has cooperated.

MR. COOK: In other words, by preliminarily resorting to these methods, you have obtained some kind of evidence against this person of a crime?

MR. SCHLAM: That is right. We would have a case against the individual, and then by the process of seeking to obtain his cooperation, tell him the advantages of cooperating with the government.

MR. COOK: Continuing to go backwards, then, what are the initial investigative methods which your cases have relied upon to obtain evidence of crime?

MR. SCHLAM: I think in our district we have an interesting situation from the standpoint of the Commission.

In looking back over the work that has been done in the Eastern District of New York since 1970, the case which I believe was the wellspring from which much of our work has developed began with a wiretap. It wasn't a Title III; it was a state wiretap.

And as a result of this case, we were able to induce one of the defendants to cooperate with us, and I think it is fair to state that as a result, directly and indirectly, we have indicted approximately 250 persons in our district, the Eastern District of New York, considered by the Drug Enforcement Administrator to be Class 1 violators, the highest classification in terms of importance to the narcotics traffic. We have convicted—of those who we were able to arrest—all but maybe two.

And all of this, I would say, sir, with few exceptions, was done primarily on the basis of accomplice testimony.

MR. COOK: You referred initially to the state wiretap. And just so that we are talking about what I think is the same case, is this what is known in the reported cases as the *Poeta* case or *Steppenber*g?

MR. SCHLAM: Yes, sir. The reporting is the *Poeta* case, because Steppenber

g died before he was sentenced. They were co-defendants.

MR. COOK: Did your office have any role in obtaining the initial state wiretap?

MR. SCHLAM: We did not.

MR. COOK: And how did it come to pass that the state authorities came to you with evidence obtained from this wiretap?

MR. SCHLAM: I think primarily it came to us because the State of New York, as a practical matter, the prosecutors and the State Police are not geared to conspiracy types of prosecutions. And the Federal Government, because of our differing laws of evidence and because of, I think—to a certain extent because of the attitude of the federal judges as opposed to the state judges—the State Police felt that the Federal Government provided a more conducive climate to bring the prosecution.

They brought the prosecution to us. We convicted both Steppenber

g and Poeta, and from there our work began.

MR. COOK: Can you briefly describe the specific differences in evidentiary laws between the State and Federal systems?

MR. SCHLAM: In New York they have what is called a corroboration requirement which, as I am sure you know, means that they have to have independent evidence aside from the testimony of accomplices or co-conspirators in order to have a legally sufficient case. In the Federal courts, we don't have that rule. Based on the testimony of one accomplice, if believed by the jury beyond reasonable doubt, it would be sufficient to convict.

So we have that big advantage.

I think also we have what I would term more psychological advantage in the sense that we are willing to bring cases which do not result in a seizure, which do not result in a buy. In fact, some of the cases we consider our most important cases were made without any narcotic evidence being offered at all during any part of the trial.

MR. COOK: And these are the conspiracy prosecutions?

MR. SCHLAM: Conspiracy prosecutions. This type of case, as a practical matter, would be unheard of in a State court.

MR. COOK: What was the state of the case when it was first presented to you by the State authorities?

MR. SCHLAM: The state of the case was that they had wiretaps which had resulted in their obtaining incriminating conversations on three of the individuals who ultimately were indicted and convicted. Additionally, they had surveillances and they had developed an informant who ultimately was a witness for the government at the trial, who testified to his relationship with the three defendants in connection with their narcotic activities.

MR. COOK: But they had not succeeded in seizing any physical evidence at that time?

MR. SCHLAM: They seized physical evidence from the witness. They had not succeeded in seizing any physical evidence from the prospective defendants.

MR. COOK: Now, have the activities of your office relative to the prosecutions of the 250-some defendants you referred to derived in total from this case?

MR. SCHLAM: Well, I said directly and indirectly, Mr. Cook, and the reason I qualified that was because our activities in this area, I think, have been successful in part because of the feeling on the part of persons who might or might not be inclined to cooperate, in other words, persons who are arrested who would be in a position to help us if they wanted to, that it paid for them to help us.

In other words, we developed credibility with persons who were, if they so desired, in a position to help us. And this credibility, I think, derived from the way the persons in the *Steppenber*g case were handled and were treated—the persons who ultimately cooperated.

Additionally, when I said directly, I meant directly major cases were made as a result of the testimony of the defendants in the *Steppenber*g case.

MR. COOK: How did this procedure specifically come about? In other words, you developed cases against 250 people arising from a single wiretap, and I take it this took place over a period of time?

MR. SCHLAM: It took place from 1971 until the present day.

MR. COOK: And did this involve the inducements of persons against whom evidence already had been obtained to further participate in criminal activities?

MR. SCHLAM: No, sir. The persons we have used as witnesses—I say the great majority, and I can't think of one who wouldn't fit within this category—are persons who are incarcerated, who are strictly witnesses as to things that happened in the past. Our prosecutions have not to any substantial extent—I am almost willing to say to any extent at all—involved the use of informants who would be active in an ongoing criminal organization. Our cases are made about things that happened in the past that the witnesses knew about and were in a position to testify about.

MR. COOK: This has constituted what is a chain reaction. Is that a correct characterization?

MR. SCHLAM: I think it is a chain reaction. I think the results showed that that part of the organization of the international narcotics traffic that we were concerned with was interrelated.

MR. COOK: Can you describe the function and role of the grand jury in this proceeding?

MR. SCHLAM: Well, as it turns out, the grand jury does not play a major part in our work. And I say that because once the witness has decided to cooperate with us, the procedure is that he will be debriefed intensively by the agents. The agents would attempt to corroborate what he says by obtaining whatever documentation or other evidence that they could, and by the time he goes to a grand jury to testify, it is merely for the purpose of giving an outline of what his testimony will be at the trial, and it is not for the purpose of compelling him to do anything that he doesn't voluntarily want to do.

He has made his decision. He is going to be a witness for the government. And the grand jury presentation is basically an outline and a skeleton presentation for the members of the grand jury so they can vote on the indictment.

MR. COOK: Now, in the sense that these have been conspiracy cases, have these ordinarily been multiple-defendant indictments?

MR. SCHLAM: I would say exclusively.

MR. COOK: And do you have any idea how many indictments have resulted?

MR. SCHLAM: It would be approximately fifty. That is an estimate, sir.

MR. COOK: You testified that the evidence which you obtained involved primarily criminal offenses which had been committed previously. Does this mean that you had no occasion to use consensual monitoring devices?

MR. SCHLAM: I cannot think of any. None come to my mind offhand.

MR. COOK: Have you had much experience with court-ordered wiretapping yourself?

MR. SCHLAM: I have had experience in three cases where wiretaps have been used, two state wiretaps and one a Federal wiretap. As a matter of fact, the case which I tried most recently, last month, involved a Federal wiretap.

MR. COOK: And have you had success in cases based on wiretap evidence?

MR. SCHLAM: Yes, sir.

MR. COOK: Based on your experiences, could you make any comparative assessment of the value of the wiretap evidence against the type of accomplice testimony and witness testimony that you obtained in the *Poeta* cases?

MR. SCHLAM: In my judgment, wiretap evidence is the most powerful evidence that the prosecution can offer in a criminal case.

MR. COOK: Did the series of investigations which resulted from the initial *Poeta* wiretap ever offer you any opportunities to install subsequent wiretaps?

MR. SCHLAM: No. And the reason for that, sir, is that, as I say, our witnesses are incarcerated, and more often than not, a period of time will elapse before they decide to cooperate with the government. So by the time they decide to cooperate, the knowledge that they had would be stale from the standpoint of obtaining an eavesdropping warrant. And that is the basic reason why I believe we have not used their information in order to obtain wiretaps.

MR. COOK: You testified that in the opinion of the Drug Enforcement Administration investigators the bulk of these defendants, if not all of them, were Class 1 violators. Have these defendants fit what you would define as organized crime people?

MR. SCHLAM: Without any doubt, sir.

MR. COOK: And given the fact that organized crime is susceptible to different definitions, would you say that these organized crime operations relate back to the five-family dominated syndicated operations in New York?

MR. SCHLAM: That is a difficult question for me to answer, Mr. Cook, for the simple reason that in the Eastern District of New York we do have a strike force in addition to a United States Attorney's office.

I believe that somewhere along the line there is a connection. I have no doubt about it. But our prosecutions would not relate to persons who would be listed members of an organized crime family.

MR. COOK: None of your defendants have included named members of the five families?

MR. SCHLAM: One individual did, and that individual was prosecuted by our office because he was one of, I believe, eight defendants who were being tried together in one trial. And because the other eight were non-members, the decision was made that we should try the case.

That is the only case that I can recall where a listed member of organized crime was prosecuted by the U.S. Attorney's office in a narcotics case.

MR. COOK: In developing the kind of evidence that you have referred to about the commission of past criminal offenses, what kind of control does the prosecutor have and what kind of discretion can he exercise in the obtaining and use of this evidence?

MR. SCHLAM: Accomplice evidence, Mr. Cook?

MR. COOK: That is correct.

MR. SCHLAM: Well, I think the prosecutor is the person who would be in the best position to control the use that was made of a particular individual who had agreed to cooperate.

Our general procedure is to debrief the individual. The agent will debrief him and then we analyze the debriefing statement for the purpose of attempting to shape an indictment or indictments that could come from this particular individual's testimony.

That would take place after attempts were made to corroborate the individual's testimony and to conduct whatever investigation was felt appropriate.

MR. COOK: The primary inducement for these individuals to testify before the grand juries and in open court, I take it, was the fact that if they did not do so they would face substantially higher criminal penalties?

MR. SCHLAM: That is correct. And this inducement is a real one in the area of narcotics, because the sentencing practices in narcotics cases is to levy stiff sentences.

The defendants know this, and I believe that that is really the main reason why we have been as successful as we have in convincing these people to cooperate.

MR. COOK: I take it in developing a credibility among these potential witnesses you have had some kind of liaison with the judiciary?

MR. SCHLAM: We have. And I think that in the Eastern District of New York, where my experience has been, we are very fortunate to have judges who are experienced with the law of conspiracy, who are in a position to try what in many cases are difficult and complex, the time-consuming, and cumbersome cases.

I give great credit to the judges in our court for the success that we have had.

MR. COOK: Have you had any experience in your district and in your experience as Assistant United States Attorney with corruption or white-collar offenses?

MR. SCHLAM: We have had, sir.

MR. COOK: Have you personally had experience?

MR. SCHLAM: I have had, sir.

MR. COOK: And have you found that the same methods which you have employed in narcotics cases have been successful in the prosecution of corruption or white-collar crime?

MR. SCHLAM: Not nearly as successful. And again I would attribute that to a great extent to the sentencing practices in narcotics cases.

My experience has led me to believe that the single thing that motivates a person, a defendant, to cooperate with the government with all its attendant disadvantages is the expectation of leniency. And that expectation becomes an increased factor to the extent that he anticipates the length of sentence that he reasonably might receive.

MR. COOK: Do you consider the *Poeta* case to be a characteristic case, the kind of thing you can expect in the future on those prosecutions, or do you think this just happened to arise from a particular set of circumstances?

MR. SCHLAM: I think one can reasonably expect that type of investigation and prosecution in any area where there is organized narcotics trafficking, which I would imagine would involve the major urban centers of the United States.

MR. COOK: Would the inference be proper that at the outset of this type of prosecution there must be either a wiretap or some type of evidence-gathering technique which is sufficient to set in motion the inducements?

MR. SCHLAM: I would agree with that, Mr. Cook, and I might add that any time that a wiretap would be feasible in any case that I were handling—and I think I speak for the other assistants in the Eastern District—I would do whatever we could do in order to try to get a wiretap. Because, as I say, there is no better evidence than a wiretap.

MR. COOK: Mr. Chairman, that concludes the staff's questioning.

Thank you very much.

CHAIRMAN ERICKSON: Professor Remington.

MR. REMINGTON: I have no questions.

CHAIRMAN ERICKSON: Professor Blakey.

MR. BLAKEY: I have no questions.

CHAIRMAN ERICKSON: I thank you for your attendance, Mr. Schlam. You have been very helpful, and I think your testimony will add to our report in determining what has been the experience with Title III.

MR. SCHLAM: Well, I was honored to be here, Justice Erickson, and thank you very much.

CHAIRMAN ERICKSON: Thank you again.

Our next witness is Mr. Thomas E. Kotoske.

MR. KOTOSKE: Good morning, Mr. Chairman, and members. It is a privilege to be here.

CHAIRMAN ERICKSON: Mr. Kotoske, will you raise your hand and be sworn.

[Mr. Kotoske was sworn by Chairman Erickson.]

TESTIMONY OF THOMAS E. KOTOSKE, ATTORNEY IN CHARGE, SAN FRANCISCO STRIKE FORCE

CHAIRMAN ERICKSON: Mr. Cook.

MR. COOK: Mr. Kotoske, your present position is Attorney-in-Charge of the San Francisco Strike Force, is that right?

MR. KOTOSKE: That is correct.

MR. COOK: And can you briefly describe for the Commission your experience in law enforcement prior to that?

MR. KOTOSKE: Prior to that time I was a member of the defense bar and personal injury attorney back in Chicago and Gary, Indiana. In '69 I came to Southern California and received a commission as Assistant U.S. Attorney in the Southern District of California and remained there, after becoming Division Chief of the Criminal Division until the first of '74, and then I received a commission as the Attorney-in-Charge of the Strike Force field office in San Francisco where I am presently assigned.

MR. COOK: What were your prosecutive experiences as an Assistant United States Attorney?

MR. KOTOSKE: Primarily in the area of organized crime, prosecutions of that nature involving Frank DeSapio, the Frontier Hotel case.

After that I left and came to San Francisco.

MR. COOK: When you were in the U.S. Attorney's office in the Central District—I take it that is located in San Francisco?

MR. KOTOSKE: The Central District is in Los Angeles.

MR. COOK: Los Angeles. Did you ever have occasion to become involved in wiretapping in that office?

MR. KOTOSKE: Yes. I think, as a matter of fact, it was one of the first—either the first or second Title III that that office handled. I personally was the supervising attorney and supervised the wiretap. After that I played a hand in and supervised primarily all the Title III's that were used in the Los Angeles area—not as the direct supervising attorney, but assisting in the assessment of the affidavits and the procedures to be followed.

MR. COOK: Now, in your position you were called upon to make assessments, I take it, of each prosecution that your office embarked upon; is that right?

MR. KOTOSKE: Mr. Cook, I personally reviewed the intake of the facts before the affidavit was written, that is, the application, and I personally approved the application that was sent back from our office here to Washington, in each and every instance.

MR. COOK: Aside from Title III investigations, do you also have occasion to review the presentation of evidence and gathering of evidence in other types of cases?

MR. KOTOSKE: Yes, I do. I personally do all of the intelligence and listing for case selection in my area, in the San Francisco Strike Force's area, which encompasses something like eight states.

MR. COOK: In addition to Title III, during your experience as Attorney-in-Charge of the San Francisco Strike Force, what other investigative techniques have you employed that are, I take it, essentially organized crime type cases?

MR. KOTOSKE: They run the full gamut, use of the grand jury, search warrants, immunities, the use of consensuals—the full arsenal of tools available to a strike force attorney, and any prosecutor, for that matter.

MR. COOK: Could you select any of these techniques as being particularly effective or comparable in effectiveness to Title III?

MR. KOTOSKE: Initially I might state I don't find any tool in the strike force prosecutor's kit as effective as Title III. There is one particular investigative device and technique that I stress very heavily, and that is the use of Kel-kits and tech's or body recorders.

MS. SHIENTAG: What is that?

MR. KOTOSKE: Consensual monitoring, if you will. I tend to stress that very heavily for several reasons. One is the rapidity of the movement, the ability to move a lot quicker than you can with the cumbersome procedures that are attendant to a Title III intercept—which can be lost in the movement of the investigation if you don't move quickly enough. I prefer that technique. It is not always available. The risk to the agent or informant sometimes outweighs its availability as a tool. But I prefer it. And I suppose I use it probably as heavily as anyone—probably more than most.

MR. COOK: Given the types of crimes that your office investigates in the organized crime field—would you characterize these offenses as being of a dynamic, ongoing, changing nature, or are they relatively stable? In other words, you refer to the rapidity of movement that is necessary for

the implementation of consensual devices. Is this also applicable to Title III?

MR. KOTOSKE: I am not sure I grasp that question, Mr. Cook, simply because I may have been thinking about something else.

If the question is: If a factual situation is so fluid that there is not the time to draft the affidavit and wait for the processing back here in Washington, and if I have an opportunity to use a consensual, I will use the consensual.

If the factual complex is static enough where I can enjoy the luxury of a few weeks, or whatever time it takes to process the application, quite obviously, because of the nature of the evidence to be derived from the Title III, I would prefer that.

MR. COOK: Directing your attention, then, to the nature of the criminal offenses which you ordinarily investigate, are these offenses ordinarily of a fast-moving, fluid nature, or can you make a judgment of that type?

MR. KOTOSKE: No, not really. On the compendium that goes from static to fluid, I couldn't say. I couldn't say that strike force types of investigations are normally one or the other.

Understand, of course, we are not case-report prosecutors. The case does not come to us in a completed form as it may to an Assistant U.S. Attorney. So the input of the prosecutor and the agent are generally ongoing with the investigations development, you see. There are certain points in time—and I am sure you are aware of this—when it is appropriate to move and move as rapidly as you can.

Is that clear or is that in response to your question?

MR. COOK: Yes, I think it is, and I think it enables us to move on into another area related to that. You referred to the cumbersomeness of Title III procedures. Can you elaborate on that?

MR. KOTOSKE: Well, the answer to that question is directly tied to prosecutorial decisions as to whether or not to use a Title III. And there is a natural culling process there that I use that makes it sometimes cumbersome.

The first two or three steps, of course, are not. They are formalistic. It is merely a grocery list approach assessing a composite of facts to see whether they fall within Section 2516.

There is the necessity of finding out whether this is the type of crime the strike force unit should be considering. Once you pass hurdles 1 and 2, you get down to the hard decision: Are there alternatives?

CHAIRMAN ERICKSON: Are there what?

MR. KOTOSKE: Alternatives to Title III. Will immunities work without tipping off the sum and substance of your investigation? Will search war-

rants work? Can the grand jury accomplish the purpose? Will consensu-als work?

And if they can, it is my judgment as a prosecutor that I will not go for a Title III if anyone of those alternate procedures can work.

If the situation develops that there is no alternative to making the case, then it becomes a dollar-and-cents proposition, the cost of a Title III versus the criminal impact.

And if I find we are pursuing a "Mom and Pop" grocery store or some \$10,000 a week narcotics operation, in my judgment the cost of the Title III—even if it gets past the first four hurdles, I would be disinclined to ask for a Title III, even prepare the application.

MR. COOK: Once you have made the decision to proceed with a Title III, are you ordinarily satisfied with the speed with which your applications are handled relative to the investigative needs which you have?

MR. KOTOSKE: I did not use to be. I am more inclined to be satisfied with the processing now.

In the formative years—I think the first case I handled was in '69 or '70, I can't remember which—we were trying to recapture a converted B-25 bomber that was being used in a smuggling operation in Mexico and coming in through Arizona and Southern California. It was very important to get on the phone at the right time. Because of delay, that case never came to fruition on that particular point, albeit it developed magnificently on another aspect.

Since that time, we have had a policy in the Organized Crime Section of response within five days of receipt of a sufficient affidavit. I think what you are referring to here is an application.

I am not disgruntled about that. I think that is a sufficient delay, I should say.

But what does bother me to some extent is the situation that has developed with some agencies, where a companion affidavit moves through the investigative agency at the same time our application is going back to the section. And I wonder whether or not that is necessary.

It seems to me there is some concomitant redundancy there we just don't need.

I can't pinpoint a case where a delay has resulted that has frustrated the objective of the investigation, but I just wonder whether that is needed. I mean, how many bishops do you need to put their imprimature on an affidavit? Four from this agency and four from our organization, when the statute only requires one?

But that is my personal feeling, and I do not speak for the Department of Justice in that regard.

MR. COOK: Have you experienced any substantial changes in the contents of your affidavits as a result of investigative agency decisions in reviewing the affidavits?

MR. KOTOSKE: Yes, I have, on at least two occasions.

But what bothers me is this, Mr. Cook. If the agency we are working with is supplying us all the facts available to them and, two, if we, as prosecutors in the field who have to live with the affidavit in front of a district judge, have made an initial determination that it is legally sufficient, and three, if the Section back here provides an added dimension or nationwide coordination and objective assessment which I have no disagreement with—I prefer it, as a matter of fact—if we go through all those steps, why is it necessary to have the same process being gone through through an agency for whom we are working?

And that, I think, is to some degree redundant. And what bothers me about it, speaking candidly, is the possibility of delay, the possibility that the agencies are not attuned to our schedule.

MR. COOK: What is the organized crime situation, briefly, in San Francisco?

MR. KOTOSKE: Well—

MR. COOK: If you give us a general assessment without revealing any of your intelligence.

MR. KOTOSKE: I would prefer not to discuss ongoing investigations, of course. I'd be foreclosed from that.

It all depends on your concept of organized crime. I am sure most people that discuss organized crime with you are confined to vowels, names that end in vowels. We have had projects going in the San Francisco area, in the Chinatown area, that have indicated to us that some of the facets of the Tongs in the San Francisco area are more effectively and sophisticatedly and efficiently organized than your standard Mafia or La Cosa Nostra could ever think about being. Whether or not they have the nationwide syndication, I don't know.

Our experience in Hawaii, for instance, has shown that the syndicate there and the criminal operative groups there are much more sophisticated, much more efficiently organized than the standard notion of the Italian organizations and Mafia or Cosa Nostra, or whatever you want to designate.

As to San Francisco itself, both the traditional organized crime families are there—they are active—as well as their companion or correlative groups, the Chinese organizations. Some of the Mexican American organizations in specific areas of criminal enterprise are at least as efficiently organized and at least as effective in their criminal

enterprise as the traditional notion of the Italian Mafia.

So, in answer to your question, "What is the organized crime picture in San Francisco?" I say to you it is at least as active as in other areas of the country that I have been familiar with.

I might point out that San Francisco is the place where I don't spend most of my time. I have from Alaska to Hawaii the entire Northwest to be concerned with. But in the San Francisco area, is what I designate as a high-activity center within my ambit of jurisdiction.

MR. COOK: Is there a pattern of criminal behavior or any particular types of offenses which dominate the crime scene in San Francisco—gambling, narcotics, extortion?

MR. KOTOSKE: No, I don't find one area of criminal activity that stands out head and shoulders above the normal common activity—your gambling, narcotics, extortion. We have had ongoing investigations into the political corruption and into the area of one of the local police departments. But I don't see one area that stands out noticeably different and distinct and with more activity.

MR. COOK: Do you find there are any investigative techniques which are particularly effective in political corruption investigations?

MR. KOTOSKE: No. The techniques are designed for the case. The selection of the technique to be used is pretty much called for by the facts. And they vary from situation to situation.

Cases can be easily made with informants, immunities, grand juries, as well as with search warrants and the other investigative techniques.

But I don't find one technique that stands out as being preferred.

Obviously, now, in certain criminal enterprises, a Title III is almost called for without question—in areas of gambling, in some narcotics enterprises, because of the nature of the tightness of the group. Sometimes in Chinatown groups and on the Islands, because of the ethnic makeup of the subjects, undercover penetration is simply impossible, where the group is too tight, and you are foreclosed from anything but a Title III if you are going to make the case.

MR. COOK: You testified that you make fairly substantial use of consensual devices.

MR. KOTOSKE: Yes.

MR. COOK: What effect would the implementation of a court-ordered system on the use of consensals have on your operations?

MR. KOTOSKE: Well, if I could go through the search warrant process locally—what I am saying is if I could retain the decision-making process locally, going before a magistrate much the same as

you would for a search warrant, with the intent of qualifications of sealing, affidavits, et cetera, I would have no objection.

But the beauty of the tool is in the rapidity of its use, the movement, the availability to it quickly. And if you have to go through a cumbersome process like your Title III application, I would strenuously object.

MR. COOK: In other words, your objection would be more to the administrative review than to the judicial review.

MR. KOTOSKE: Yes, I would have no problem with the judicial review, although I don't think it's necessary. Legally I don't think it is necessary. If the informant who is wired during a conversation could testify to it anyway, it seems to me to seek a search warrant is going to require a magistrate to do something he doesn't have to do in the first place.

But if I had my choice, I would prefer to have the decision-making process locally with a senior prosecutor.

MR. COOK: Do you find there is a substantial percentage of your consensual devices which you use under circumstances in which you do not have probable cause?

MR. KOTOSKE: Yes; yes.

MR. COOK: Under those circumstances, you could not obtain a warrant?

MR. KOTOSKE: True.

MR. COOK: I see.

MR. KOTOSKE: Without a doubt.

MR. COOK: Excuse me?

MR. KOTOSKE: I finished.

MR. COOK: I just have one further question, and it is open-ended.

When we talked to you in San Francisco, you emphasized very heavily the importance of prosecutorial discretion in handling investigations and I have attempted to cover that in the questioning so far. If there is anything which has been left out or which you would like to expand upon, please do so.

MR. KOTOSKE: No, just a short addendum.

Having been a prosecutor only five or six, maybe six-and-a-half years, and having had some considerable experience with Title III's, I would simply state to you that it is probably the most effective tool that I have used as a prosecutor in case development. I think it should be used very niggardly and with the right set of facts, with the anticipation of serious criminal impact—simply because of the cost, simply because there may be easier ways to do it, and because of the cumbersome procedures that one must go through to secure it, to secure approval of the application and ultimately the order.

With that, that is all. I think I have covered primarily the prosecutive decision-making process.

MR. COOK: Thank you very much.

Mr. Chairman.

CHAIRMAN ERICKSON: Judge Shientag.

MS. SHIENTAG: Thank you, Mr. Chairman.

Mr. Kotoske, you testified that the cumbersome procedure is what turns you off from using a Title III wiretap. Would you suggest a less cumbersome way of achieving that result?

MR. KOTOSKE: Yes, I can, Madam.

One, initially I think the procedure—the control mechanism is really what it is. I am sure you are all aware of that procedure—to be very certain that some prosecutor doesn't go off half-cocked, spending a lot of time and effort in the area.

I think it was also designed for the careful development of the statute and case law.

I have no objection to that. I have no objection to the review back here in Washington. My only objection is (a) I don't see the need for agency review, concomitant with section review, ours, and (b), I object very strongly to the time delay between the time I submitted an application and got a response.

Let me interject something there.

While the affidavit may seem very complete and the facts very static, things can happen in the meantime. Innocent things can happen. A man can sell his location. He could have it on the market. Two officers could come into a bar and have lunch, and that could be interpreted in a thousand different ways.

So my objection is this: The procedure is cumbersome. I don't object to the within-the-section review, but I do object to the out-of-section review.

I have no suggestions how you could eliminate—

MS. SHIENTAG: You do or you don't have?

MR. KOTOSKE: I do not. And I might seem to be talking inconsistently here, but some of that control mechanism is absolutely necessary for nationwide coordination.

MS. SHIENTAG: When you were the head of the Criminal Division of the U.S. Attorney's office, did you have such agency review as you have now as head of the Strike Force?

MR. KOTOSKE: You know, at that time I think Mr. Petersen was doing it himself. I used to talk to him on the phone about it, if I recall. And I don't recall that extensive agency review was going on. As a matter of fact, if I recall that first case, there was not. It was all done within the section.

Has that answered your question?

MS. SHIENTAG: Well, I think we all appreciate that when a procedure is comparatively new, as this is, we want to be sure the rights of everybody, the

defendants and people and government, are protected. So it may be necessary to follow certain procedural steps as safeguards.

As we become more familiar with the process of getting Title III authorizations, perhaps there are some things that could be eliminated. That experience has shown. That is the purpose of our asking you these questions now.

If you find there are some specific agency reviews which could be eliminated based on your experience, which is extensive over the last six years, would you submit that to the Commission?

MR. KOTOSKE: Sure.

MS. SHIENTAG: In other words, would you review your files and indicate specifically how something could be shortened, made less expensive, and you would achieve the results?

MR. KOTOSKE: I'd be very happy to do that.

MS. SHIENTAG: Thank you.

CHAIRMAN ERICKSON: Does that complete your questioning?

MS. SHIENTAG: Yes. Thank you, Mr. Chairman.

CHAIRMAN ERICKSON: Professor Remington?

MR. REMINGTON: I have no questions.

CHAIRMAN ERICKSON: Professor Blakey?

MR. BLAKEY: I have no questions.

CHAIRMAN ERICKSON: General Hodson?

MR. HODSON: You indicated that there, at least, is some type of organized crime activity around the San Francisco area. We understand Alameda County has a fine police force and a fine prosecutor's office, but they don't have wiretap authority at the state level.

MR. KOTOSKE: That is true. California does not.

MR. HODSON: Do you have any comment to make with respect to their capabilities in combatting organized crime without wiretapping?

MR. KOTOSKE: General, only in this regard—let me say two things. Let me say one thing generally, and then more specifically with respect to Lowell Jensen's office, who is the District Attorney there. And I agree with you, they do have a very fine police department there.

MR. HODSON: And he has a fine reputation as a prosecutor.

MR. KOTOSKE: An excellent police department, and Mr. Jensen is now at trial, as you know, on a very complicated case.

One, my experience indicates to me, for whatever it is worth, that states who do not have the authority to intercept on the line, who do not have wire intercept authority, will never be able to come to grips effectively with organized crime, simply because organized crime, in order to do its busi-

ness, needs the wire. If you do not have access to control of that particular facility, you are always going to be two steps behind. I am not aware of any bills presently afoot in the California Legislature for statutes like Title III. Until that occurs, they are always going to be just one step behind the problem.

MR. HODSON: You have a feeling that you are picking up the stick, so to speak, in the organized crime area from the state authority?

MR. KOTOSKE: Not necessarily, General. Given the small size of the Federal family, it is generally impossible to effectively conduct a Title III investigation without the help to some degree of the locals, its PC input, manpower surveillance, or commitments, not to the in-house operation, but a myriad of things that have to go on during an investigation. I have personally never handled a Title III where there was not some local cooperation.

I do not intend to convey to you the idea that the locals feed us with facts, hoping we can develop them into a Title III case, albeit that frequently happens. But I don't think it is in the sense of picking up the sticks and doing something the state law enforcement could not otherwise do.

Sometimes that does happen.

I can give you two cases, the recent case in Hawaii and the recent case in San Francisco, both Title III cases and very extensive, where local cooperation was absolutely necessary. And I draw very heavily where I can on local law enforcement to assist.

MR. HODSON: Let me just ask you one question here about criteria for wiretapping.

You indicated your criteria—

MR. KOTOSKE: That is very subjective.

MR. HODSON: —part of which was a cost-effectiveness analysis. Have you ever had a case turned down by the Department of Justice on the basis that they did not consider it important enough to use Title III?

MR. KOTOSKE: No.

CHAIRMAN ERICKSON: I just have a few questions, Mr. Kotoske.

You have a number of states on the West Coast that you are in charge of as far as the Organized Crime Strike Force is concerned. Except for California, do any other states on the West Coast fail to have companion legislation that would prohibit state wiretaps in law enforcement?

MR. KOTOSKE: I am disadvantaged, Mr. Chairman. I know California does not. I believe Oregon does.

CHAIRMAN ERICKSON: It does.

MR. KOTOSKE: I think Alaska does. I know Hawaii does not. I don't know about Montana, Idaho, and Utah. I don't have that information; I'm sorry.

CHAIRMAN ERICKSON: But in connection with these states, have you ever turned to a state for assistance in obtaining a wiretap because of the fact that their procedures were less cumbersome than the Federal procedures?

MR. KOTOSKE: No, sir; I never have.

CHAIRMAN ERICKSON: Do you feel that this requirement of being checked at all these levels is essential to protect privacy or make certain that wiretaps are only issued in the most aggravated case, if you will?

MR. KOTOSKE: Yes. I have no objection to the procedure as long as it remains in-house. By that I mean, as long as the review process—which I think is absolutely necessary—as long as the review process remains within the Organized Crime Section solely.

What I object to—and I think I was making this point earlier—is the out-of-section review that I think is redundant and unnecessary. And I know people disagree with me on that point.

CHAIRMAN ERICKSON: Well, what I was aiming at was: Do you feel it is necessary to do that rather than have the determination made at the

local level as to whether or not this will be pursued?

MR. KOTOSKE: I think the review process is necessary to protect the statute from abuse. I disagree—and I might also say I do not think that I or any other senior prosecutor ought to make the decision at the local level in connection with Title III's.

I do object to the redundancy that seems to be apparent with this companion review going on at the agency level.

CHAIRMAN ERICKSON: Those are all the questions I have.

Are there any further questions?

[No response.]

If not, Mr. Kotoske, we appreciate your appearing. Again, you have been most helpful.

MR. KOTOSKE: It has been my pleasure, Mr. Chairman.

CHAIRMAN ERICKSON: Thank you again for coming.

This meeting stands recessed.

[Whereupon, at 12:50 p.m., the meeting was adjourned.]

Hearing, Monday, June 9, 1975

Washington, D.C.

The hearing was convened at 9:30 a.m., in Room 6202, Dirksen Building, Professor J. Remington, Chairman pro tem, presiding. Commission members present: Frank J. Remington, Chairman pro tem; Richard R. Andersen, G. Robert Blakey, Florence P. Shientag.

Staff present: Kenneth J. Hodson, Esq., Executive Director; Milton Stein, Esq., Michael Lipman, Esq., Margery Elfin.

PROCEEDINGS

MR. REMINGTON: I think we are ready to commence today's hearing.

I will recognize first General Hodson, who has a motion or two to make.

MR. HODSON: Mr. Chairman, I suggest that the staff reports on the state and local law enforcement from the Los Angeles and Chicago areas be made part of the record.

MR. REMINGTON: Without objection, they may be made part of the record.

PROFESSOR BLAKEY: Mr. Chairman, I enter my continuing objection that these reports are not comprehensive enough. But I don't object to their being received for the record.¹

MR. HODSON: Second, Mr. Chairman, I suggest the letter we received from the District Attorney of Philadelphia, Mr. Emmett Fitzpatrick, be entered in the record. We invited Mr. Fitzpatrick to appear because he comes from a major metropolitan area where they do not have court-ordered wiretapping. Mr. Fitzpatrick declined on the grounds that he has had no experience with the use of electronic surveillance and therefore he has had no occasion to get involved with it, and therefore he declined our invitation.

MR. REMINGTON: Without objection, the letter from District Attorney Fitzpatrick will also be made part of the record.

[The letter referred to above follows.]

DISTRICT ATTORNEY'S OFFICE
PHILADELPHIA, PENNSYLVANIA

April 30, 1975

F. EMMETT FITZPATRICK
DISTRICT ATTORNEY

¹ Staff reports are published in a separate volume.

Mr. Kenneth J. Hodson

Executive Director

National Commission for the Review of Federal and State Laws
1875 Connecticut Avenue, N.W.
Washington, D. C. 20009

Dear Mr. Hodson:

I am in receipt of your letter of April 24. Unfortunately, it appears that I am unable to help you.

I have been District Attorney but shortly over a year. During this period of time, wiretapping has been illegal in the Commonwealth of Pennsylvania and our legislature recently passed a prohibition against bodytaping as well.

I have not had occasion, therefore, to become involved with electronic surveillance in the development of any criminal matters. I do note, however, that the Special Prosecutor, Mr. Walter Phillips, has expressed some interest in these activities. You might wish to contact him directly and determine the status of his activities in these areas.

Sincerely,

[Signed] F. EMMETT FITZPATRICK

MR. REMINGTON: As members of the Commission know, we have heard testimony from a number of persons active in law enforcement in New York City, the only large city which has court-authorized electronic surveillance authority as a matter of state statute. And in that testimony we have heard from New York City Prosecutors and law enforcement personnel that they rely heavily on the authority which they have to conduct electronic surveillance.

In this hearing today we will have the advantage of being able to hear from experienced and knowledgeable representatives of law enforcement in the next three largest cities, Chicago, Los Angeles, and Philadelphia, who will discuss with us their view as to the need for court-authorized electronic surveillance in their jurisdictions, the present situation being that there is no authority under state statutes in California, Illinois, or Pennsylvania to conduct electronic surveillance.

We start this morning with District Attorney Joseph Busch from Los Angeles County, the largest county in the United States. Anyone who knows anything about law enforcement in this country knows the distinguished record of Mr. Busch, who has been District Attorney for Los Angeles County for 20 years and presides over an office that is known for its competence and ability, and it is therefore very pleasant for all of us to be able to hear the views of Mr. Busch this morning.

Mr. Busch, the rules of the Commission require that all persons appearing before it be sworn.

[Whereupon, Joseph P. Busch was duly sworn by the Chairman pro tem.]

MR. REMINGTON: Mr. Busch, we welcome you this morning.

MR. BUSCH: Thank you, Mr. Chairman.

MR. REMINGTON: We understand you are going to start with a statement. We have copies of your written statement and without objection that will be made part of the record.

TESTIMONY OF JOSEPH P. BUSCH, DISTRICT ATTORNEY, LOS ANGELES COUNTY, CALIFORNIA

MR. BUSCH: I am Joseph Busch. I am District Attorney of the County of Los Angeles.

It is an honor to meet with you today and to discuss a topic which has become increasingly important to all Americans—wiretapping and electronic surveillance.

The uses and abuses—both private and governmental—of the technological tools for eavesdropping have become of great concern to millions of people. Those who have been the subjects of illegal or misdirected electronic snooping are understandably bitter. Millions who have only heard about the techniques used or who only suspect that their private conversations may have been listened to are almost equally angry.

People both in and out of government who were concerned about such intrusions on personal privacy applauded the controls set forth in the Federal electronic surveillance law. Both as a public lawyer and as a citizen, I personally welcomed the standards established by this act.

In the present assessment of this law which your Commission is undertaking, I wish to address you as a public lawyer from a state which prohibits non-consensual electronic wiretapping and eavesdropping by law.

Before we get into questioning, I want to discuss with you briefly some of the problems which develop for investigators as a result of such a total ban and touch briefly on possible further restrictions on consensual electronic surveillance which is used continually by the Los Angeles District Attorney's Office and other law enforcement agencies in our jurisdiction.

The office which I head is the largest prosecutor's office in the nation and serves an area which is larger than forty-four of the states. We handle all the felonies and about half the misdemeanors which occur in our jurisdiction—about 250,000 cases a year.

In addition to our legal staff of 520 attorneys, we have a Bureau of Investigation of 300 investigators, the third largest police agency in Los Angeles County.

The Bureau of Investigation works closely with two legal units most closely involved in electronic surveillance—the Organized Crime and Narcotics Division and the Special Investigations Division. As its name indicates, the Organized Crime and Narcotics Division is concerned with organized crime, which we define as ongoing criminal conspiracies, and the organized narcotics traffic in our area. The Special Investigations Division deals mainly with government corruption, bribery, and election frauds.

Consensual electronic surveillance is used most frequently by the Special Investigations Division in cases of government corruption and bribery. We consider them essential in this most important area of prosecution. They are an essential electronic verification of the testimony of our witnesses who are often in a one-on-one situation with the suspect, especially in bribery cases.

In certain organized crime cases, including a recent murder-for-hire case, consensual surveillance has been critical to the success of the case.

In another major case recently involving the theft of millions of dollars of city checks which is still pending trial, consensual electronic surveillance was also critical. And this particular case clearly reveals the problems which would arise if the law is changed to require court orders for consensual electronic surveillance.

The scenario for our effort to recover some of these checks changed literally on a minute-by-minute basis. For hours, our investigators and attorneys were making constant adjustments in the time, place, and manner in which the checks would be received by our informant.

If court approval had been required for the electronic surveillance aspect of this operation, it would have rendered such surveillance impossible. And we had to have the surveillance.

The same type of situation also frequently occurs in bribery and government corruption cases.

These are some examples of why consensual eavesdropping is relied on so heavily by local law enforcement agencies in Los Angeles.

Before continuing, I should probably take a minute to describe the organized crime problem which we face in the Los Angeles area, how we deal with it, and how the inability to wiretap without consent affects our efforts.

The traditional organized crime reliance on a working relationship with police and public officials through bribery and other types of pressure, including political, has never existed in Los Angeles. The reasons for this probably include a highly-developed civil service tradition in local and state government, a relatively loosely structured partisan

political system springing from a tradition of cross-filing and non-partisan local elections, and a heterogeneous suburban social climate.

This does not mean that Los Angeles does not have organized crime nor that it is not a target for organized crime. It simply means that the structure of organized crime in our area is different—as are many other aspects of life in Los Angeles.

We do have bookmaking, prostitution, fencing, murders for hire, narcotics, labor racketeering and the other social ills that organized crime fosters.

We are also most concerned about the movement of organized crime money into legitimate businesses in our area.

It is our opinion that the inability of law enforcement to wiretap non-consensually gives organized crime figures a sense of security and makes our area more susceptible to invasion by organized crime.

In many areas of organized crime activity, we can only arrest the lower echelons. For example, in bookmaking, we can hit the front offices, but we cannot get to the back offices or beyond due to our inability to wiretap non-consensually. As one of my organized crime attorneys noted, it is similar to going after a large corporation on a major consumer or antitrust violation and simply arresting the salesmen. We are forced to strike against the most easily replaceable elements of the organized crime effort.

It is really conjecture as to what exactly non-consensual wiretapping would do in such a situation since we don't have it. We only know that the Federal Government's ability to do such wiretapping allows them to make cases in this field that we cannot.

Virtually all the major Federal Strike Force cases that are being made in the Los Angeles area are being made with wiretaps. A recent trial of allegedly major organized crime figures for a syndicate-style bookmaking takeover relied heavily on wiretaps, for example. It is most difficult for us to tackle this kind of case.

This fact raises an interesting problem. Does this mean that in non-wiretap areas, such as California, the local agencies must come to depend on the Federal Government for the prosecution of major organized criminal activity? Does this presage the growth of a national police force as opposed to our tradition of local law enforcement control—due to the wiretap constraints placed on local agencies and the ability of the Federal Government to move in the area?

We know already that it has resulted in local agencies turning over cases to the Federal agencies, because the local agencies knew that non-consensual wiretaps were needed.

I have mentioned a recent murder-for-hire case in which consensual wiretaps were essential to the successful prosecution of the case. In another such case, our inability to make non-consensual wiretaps prevented the prosecution of the higher-up responsible parties.

We received information that a prominent local union official was the object of a contract for murder. Our informant had been asked to obtain a hit man. Conversations between our informant and the suspect who was seeking the hit man were recorded. Incriminating comments by the suspect were recorded.

Our investigators knew that the suspect would make telephone calls from a public pay telephone to unknown persons after he had talked to our informant. If we had been able to tap that phone, we believe that we would have discovered who the suspect was working for. As it was, we were never able to determine who had ordered the murder. The suspect wouldn't talk.

The narcotics problem is one which I believe needs special attention when discussing the wiretapping problem.

Los Angeles, today, is the heroin capital of the world. This has resulted from our geographical proximity to the Mexican heroin producers, the traditional ties between dealers in our area and the Mexican producers and the at-least-temporary drying up of the European sources of heroin.

The narcotics experts in the District Attorney's Office estimate that there are today 500 major narcotics dealers in the Los Angeles area. They define major dealers as suppliers who deal in large kilo amounts of heroin and cocaine. This means that the major suppliers outnumber the Federal DEA agents in the county by more than four to one. This may give you some idea of the problem which we face. As in other areas of organized crime, the lack of non-consensual wiretapping greatly inhibits our ability and that of other local agencies to get to the major suppliers and increases our reliance on the Federal efforts.

A current case in our office illustrates this problem. We know from an informant that a major dealer has a tie-in with a prominent businessman on the distribution level. As a result of the informant's activities, we were able to make a major drug seizure and will probably be able to make a case on the dealer. But the lack of wiretapping capability prevents us from reaching the businessman confederate.

That is not a unique case. It is not unusual for us to make such arrests—taking one dealer and leaving untouched his wealthy associates who lead presumably legitimate lives.

There is one other aspect of the situation in California in which I know the Commission is interested. As a result of the *Jones* decision by the California Supreme Court, 106 *Cal. Rptr.* 749 (1973), California prosecutors cannot use evidence obtained from a lawful non-consensual wiretap conducted by another jurisdiction, such as the Federal Government. Moreover, a conservative interpretation of this ruling by some authorities believes that it may even preclude California law enforcement participation in investigations by other jurisdictions when legal non-consensual wiretapping is undertaken. I personally do not agree with this latter interpretation. However, I am sure you can see the restrictions which result from this court ruling.

I should also mention that all state efforts at legislation to provide for court-approved non-consensual wiretapping have met defeat in Sacramento. Such legislation which has been sponsored by the California Attorney General's Office and local district attorneys has been highly restrictive, actually beginning where the Federal Government leaves off in terms of restrictions.

If the picture that I have painted seems dismal, I must tell you that it is probably not as bad as it sounds in this abbreviated presentation, but it is certainly not inspiring to the attorneys and investigators who must deal daily with these restrictions.

I hope that the California picture will improve and I hope that your deliberations on the Federal law will be aided by my presentation here.

I think it is naive to believe that law enforcement does not need wiretapping. I am in total agreement with the people who fear the abuse of wiretapping, and I strongly favor all reasonable steps which must be taken to prevent such abuse.

But organized crime does use the telephone; the leaders of organized crime are susceptible to successful prosecution based on the use of electronic surveillance; and as a local prosecutor who cannot use non-consensual wiretapping, I can tell you that it makes a difference.

Thank you for the time you have given me to present my views and if you have any questions, I will be happy to answer them.

MR. REMINGTON: Thank you very much, Mr. Busch. I think General Hodson would like to start with a few questions.

MR. HODSON: Mr. Busch, you made a very thorough statement covering most of the questions that I have.

I would like to have you put on the record your own biography in brief, if you will.

When did you join the Office of the District Attorney of Los Angeles?

MR. BUSCH: I joined the Office of the District Attorney in February of 1952. I did the usual type of misdemeanor training and preliminary work, and then in 1954, became a Senior Trial Lawyer and served as a Senior Trial Lawyer until 1966, when I became the supervisor of the trial lawyers in the District Attorney's Office and then, through additional promotions, became the Assistant Deputy District Attorney.

MR. HODSON: Are the Deputy and Assistant District Attorneys in the Office of the District Attorney appointive positions?

MR. BUSCH: All but two of the Deputy District Attorneys in Los Angeles are Civil Service.

MR. HODSON: Career people?

MR. BUSCH: Career people.

MR. HODSON: That leads to my next question. Do you have much personnel turnover in your office?

MR. BUSCH: No. As a public law agency, the turnover in the office is small. It gets smaller as the years go by. I would say it is about 8 per cent per year.

MR. HODSON: About 8 per cent per annum?

MR. BUSCH: Eight to 10 per cent.

MR. HODSON: Roughly, what percentage of the trial attorneys in your office may have more than three years' experience?

MR. BUSCH: Well, I would say that of the 520 lawyers that we have, all but perhaps 150 would have that much experience—350 or so.

MR. HODSON: In your testimony you indicated you rely extensively on consensual wiretapping. You indicate, also, that you would not favor a court-ordered system for consensual wiretapping.

Would you please tell the Commission what controls you place over consensual wiretapping, not only with respect to when they can be conducted but with respect to what controls you place over the equipment?

MR. BUSCH: Generally in the consensual type of wiretapping the only two methods that give you good results are a Fargo transmitter or an induction coil with reference to consented telephone conversation. All this business about the great new methods they have on electronic eavesdropping I don't find effective at all. I think that is more "007" talk than it is practically true.

The manner in which it is done is that, in my case where there is going to be consensual use of an eavesdropping device, the matter is brought to the attention of one of our Deputy District Attorneys. It is generally in the field of organized crime, narcotics, or political and governmental corruption.

The control of the industry is under our Crime Laboratory Technicians and they, of course, take

care of that. The matters, if at all possible, are reduced to a recording on a tape so that it is always available from start to finish.

As to the person that we use who may be using the Fargo, any undercover cop or whoever he may be, we try as best we can to have him under visual observation at all times with reference to it.

All of the tapes that are used in any type of consensual operation are saved. In California we have complete discovery. The prosecution turns over everything but its work product—and nowadays I am not so sure we don't have to turn over our work product—but we just open our files and save all that and make it available to the defendant on indictment so there is no destruction of the evidence and it is maintained in the regular course of the booking procedure, sealed with sealing tapes and marked by the persons who are involved.

MR. HODSON: Do you have a regular written policy with respect to controls on your electronic devices and also with respect to who may authorize the use of those devices?

MR. BUSCH: I don't believe that is actually put in writing as part of our regular office manuals. I must say that we have volumes of office procedures. But I don't believe that it is put in writing. It is a matter of general policy that we have used over the years.

MR. HODSON: You gave an example to illustrate that court-ordered consensuials would not work because of the rapid change of the situation and the movement of the witness. Was that example a typical case?

MR. BUSCH: I think that is very true. When you are dealing with a hot case and you have your men in the field and they've got—I think they like to call it the rabbit—when you have your informant walking in and out and making the contacts and keeping them under surveillance, you have to do that unless you want to take a judge along with you and let him watch. Because even under surveillance, as you know—if we put an informant in an automobile and put him under surveillance, that takes three cars, so they don't know they are being followed. It is a very involved investigative technique. You have to have communication between parties. And if they decide not to meet at one hotel and meet at another hotel, maybe you are even using the Fargo transmitter and things change right as they go along.

MR. HODSON: Do you feel, then, the controls you put on the use of consensual devices are adequate?

MR. BUSCH: Oh, absolutely. I feel this, that when we are talking about consensual we are talking about one of the parties to the conversation, to the transaction, and the control factor is there. As I

say, the destruction of the evidence I think would prove disastrous in California if we didn't have the adequate controls we do. The failure to produce that kind of evidence on behalf of the defense on discovery I think would make the case fail.

MR. HODSON: The critics of wiretapping have made a point that in the Federal agencies, at least, they use wiretaps a higher percentage of the time in gambling cases; that the gambling cases are frequently minor gambling cases and it is a waste of the use of wiretapping authority to use it in such cases.

Now, you can't use it in such cases and you indicated in your statement that you are not certain just what you would get.

The question I would like to ask you is: Do you feel gambling is important enough to use court-ordered wiretapping and thus invade the privacy of a great number of people?

MR. BUSCH: I certainly do. This idea of invading the privacy—one of the things that is intriguing is that through a proper showing we can get a search warrant and we can go into lawyers' offices and doctors' offices; we can search privileged papers and look at things and seize things under proper court order that have been reduced to writing. And yet for some reason they feel there is a different kind of invasion of privacy when we seize the spoken word that is also being dissipated and disappearing, that would be as important as anything that was reduced to writing. And actually all we are doing is reducing to a sound device the actual words being spoken so that they aren't lost in the atmosphere.

And particularly in gambling—I don't know how other areas work their bookmaking operations, but sports action and bookmaking is big business. And it isn't tough to get a disgruntled wife to turn over the phone number that her husband has been putting some bets in on to the local front office and put a phone call in and make an arrest there. But you people know you can have ten front offices and the back office is the one you want, because they are phoning in and keeping the records and keeping all of the information. And in the ten front offices they don't even know who they are working for, because all they can do is respond when that phone rings. And once you get two or three of the front offices the only way you are going to get the back office is to have a court-ordered wiretap, or else you won't get it. That is why it is so hard to bust up gambling rings.

The best operation I have seen was in Kings County, Brooklyn, where they have court-ordered wiretap and knocked off the biggest bookmaking operation I have seen in organized crime.

MR. HODSON: In prior testimony we have had suggestions that the solution to this is to legalize gambling.

Do you have any comments in that regard?

That is on the basis that people are going to gamble regardless of what you do.

MR. BUSCH: Well, from the information that we have had, I don't believe that even off-track betting is being handled as well as they would like. You are not going to run organized crime out of the gambling business by legalizing gambling. If you don't believe me, go to Las Vegas and look at it. You can gamble there and if you don't think that is part of organized crime—I just don't think legalized gambling is going to solve the organized crime problem.

MR. HODSON: Let me go to another subject. You mentioned several investigative techniques including, of course, the rather widespread use of consensual electronic surveillance. And you mentioned undercover agents and implied also that you use informants. You didn't mention anything about an investigative grand jury and the use of immunity in order to get people to testify before the grand jury and convict them of either perjury or contempt.

And in the sample case you gave, you said you were unable to go up the ladder because he refused to talk.

MR. BUSCH: That is right. Let me say, one, we don't have immunity in California. We don't have investigative grand juries. Our grand juries are not used very much for criminal purposes. They perform a watchdog function. In our county, if we have from 90 to 100 indictments a year out of the 35,000 or 36,000 felonies we actually file, that would be a lot. They cannot have ongoing investigative techniques. If a person is a suspect before a California grand jury, you don't even subpoena him; you invite him. Because if you subpoena him and have him testify, the issue is raised that you have indirectly, by compelling him to appear before the grand jury under oath, offered him immunity.

So we have to be very careful about the manner in which we do it.

Yes, we can offer witnesses immunity before the grand jury, but it is transactional immunity and it leaves us at a little bit of a disadvantage if one of the main characters is involved. Our grand jury system in California is probably a little different from most others.

MR. HODSON: In that you do not use the investigative grand jury or you cannot use it?

MR. BUSCH: The problem is, as I say, when you get a suspect—if you are going to have a possible defendant in an indictment, you invite the person;

you don't subpoena him. Because if we subpoena him we run across the problem that his testimony might have been coerced in an investigative-type technique, like the Federal Grand Jury does. And therefore the effectiveness of the grand jury as an investigative tool in the state grand jury system in California is almost absent.

MR. HODSON: Do you, in light of the *Jones* case which you mentioned, continue to cooperate with the Federal Strike Force and Federal authorities in the Los Angeles area?

MR. BUSCH: Oh, yes. On the Strike Force—it has been there for a number of years, but in the initial undertaking we always had a man assigned and available to work directly with the Strike Force. And we continue to do that. We have an excellent relationship with all of the Federal agencies in our particular area.

As a matter of fact, I think the only cases that the Strike Force has made in the Los Angeles area—I am talking now about the Los Angeles area; they have had other cases that involve areas other than Los Angeles in that Strike Force—originated from local authorities, turned over to the Strike Force because of the availability of wiretapping and the ability to use an investigative grand jury.

MR. HODSON: Have you taken any steps or established any policy with respect to cooperation with the Strike Forces when they are using electronic surveillance so as not to taint any derivative evidence that you might obtain?

MR. BUSCH: No, we don't actually participate in any of the cases that they undertake where they use electronic surveillance, because of the *Jones* case. It is sort of a strange situation, because under the Federal rules, you can even impeach a witness with legal wiretaps. So California has some crazy rules that most of the other jurisdictions aren't confronted with.

MR. HODSON: What are the basic arguments used by the critics of court-ordered wiretapping in California to prevent it from becoming law?

MR. BUSCH: Well, generally speaking, they say that you cannot restrict the scope of the wiretap to where it is not an invasion of the privacy of the individual involved. In other words, if you are going to do it for a period of time, whether it is days or hours or weeks, or perhaps 30 days, whatever it may be, then during that period of time you will be made privy to conversations that perhaps have nothing to do with the investigation, and therefore it becomes an invasion of the privacy of the individual.

But you are only seizing, in my opinion, that which would be investigative and material and relevant in a court of law, so the rest of it is just like the

papers in an office; you only seize that which is relevant.

But we haven't been able to sell that to our Legislature.

MR. HODSON: Mr. Chairman, that concludes my questioning.

MR. REMINGTON: Mr. Blakey?

PROFESSOR BLAKEY: Mr. Busch, you said that you do not use the investigative grand jury in California in part because the immunity is automatic?

MR. BUSCH: Well, it raises a question, you see.

PROFESSOR BLAKEY: If you selected your witnesses beforehand as "witnesses" rather than as "suspects," why couldn't you call them before your state grand jury?

MR. BUSCH: Oh, you could. There is no question about it. Another thing is that our grand juries were supposed to be—when you undertake an investigation it is supposed to be towards the indictment of individuals, not just on fishing subpoenas.

PROFESSOR BLAKEY: Could you quash a subpoena under California jurisprudence on the grounds that it was not directed towards an indictment?

MR. BUSCH: I think they could raise that issue. Whether or not we would fight that—yes, we would fight it.

PROFESSOR BLAKEY: If an indictment was returned after a long grand jury investigation, during the course of which you didn't have an indictment in mind, would that be grounds for quashing the indictment?

MR. BUSCH: They would raise that issue. We would object to it.

PROFESSOR BLAKEY: How do you think it would be resolved?

MR. BUSCH: In California now with an indictment, in our grand juries all testimony must be recorded. And if an indictment is returned, it must be printed up and it must be given to the defense so that they have a complete record. And then, in order to move to set aside the indictment, we would move on the grounds that there was no legal evidence to sustain the indictment, relevant legal, admissible evidence. They may move to quash it on the grounds that it was an ongoing investigation and without any particular indictment in mind, that it was being used as a prosecutor's tool, as a Star Chamber proceeding, and that type of thing.

PROFESSOR BLAKEY: Is that a ground for dismissing an indictment in California?

MR. BUSCH: These are grounds that they have raised. They have not been successful. However, there has been success in the area of having

suspects who are indicted, who are called in as witnesses under subpoena, who are forced to testify, who are not given their rights, but just as witnesses, that their testimony was coerced.

PROFESSOR BLAKEY: So I take it your testimony is that for these, among other reasons, you have no investigative grand jury program?

MR. BUSCH: It is not an effective tool.

PROFESSOR BLAKEY: It is not an effective tool as you use it?

MR. BUSCH: The way that we are restricted, it is not an effective tool such as a Federal Grand Jury that you impanel for one specific purpose and keep for a year just to go into one general area.

PROFESSOR BLAKEY: I am troubled, Mr. Busch. I am still trying to figure out why it is not. Is it or is it not the law in California that you may quash an indictment because the grand jury was used as an investigative tool rather than—

MR. BUSCH: It could be a ground. Once an indictment is returned—

PROFESSOR BLAKEY: May I break in? It could be a ground. Is it or is it not?

MR. BUSCH: It would not be, in my opinion.

PROFESSOR BLAKEY: If it is not, in your opinion, why don't you use them as investigative tools?

MR. BUSCH: Because if we indict one of the witnesses we call who had been subpoenaed—

PROFESSOR BLAKEY: Forget the witnesses.

MR. BUSCH: That is an important part of it.

PROFESSOR BLAKEY: Let's suppose for a minute you have a target and you are willing to call people in to make a case against your target. Taking your labor racketeer case, I assume your objective was not the man your informant was dealing with but ultimately the man he was dealing with?

MR. BUSCH: Yes.

PROFESSOR BLAKEY: Would it have been possible to have asked the middle man in and asked him to testify against the ultimate man?

MR. BUSCH: You mean immunize him and hold him in contempt until he testified?

PROFESSOR BLAKEY: Yes.

MR. BUSCH: Sure, it would, but he refused to cooperate in any way.

PROFESSOR BLAKEY: So you made the practical judgment that he wouldn't have cooperated anyhow?

MR. BUSCH: Yes.

PROFESSOR BLAKEY: Why wouldn't that, as an investigative tool, be open to you in all your prosecutions?

MR. BUSCH: It would.

PROFESSOR BLAKEY: The next question is: Why isn't it routinely used in Los Angeles?

MR. BUSCH: Again, what you want to do is say, "Okay, let's let this guy go. Give him immunity. Let's take this guy and let him walk free."

I don't look at it that way. I don't buy pigs in a poke. I don't look for contempt orders as producing good results. I never have.

PROFESSOR BLAKEY: The Federal people do and get good results.

MR. BUSCH: Good results?

PROFESSOR BLAKEY: I take it you don't agree?

MR. BUSCH: I don't agree with that.

PROFESSOR BLAKEY: What I am getting at is: It is a policy, not a legal judgment—

MR. BUSCH: It is also legal.

PROFESSOR BLAKEY: —that what you have to do in an investigative grand jury is something you are unwilling to do.

MR. BUSCH: Oh, no, it is also a legal problem. If you would give us use immunity—not you, but if we had use immunity, I could see a lot of benefit out of all this.

PROFESSOR BLAKEY: I am certainly willing to associate myself with your feeling that it would be better if we had use immunity, but I am also familiar with the New York practice. They have investigative grand juries and they have transaction immunity and they use them continuously to investigate organized crime cases, apart from wiretapping, where they pick people who are lower echelon people and trade them to get upper echelon people. And they make the policy choice that that is a worthwhile trade. There is nothing in the New York law that is inconsistent with it and there are some people who feel it is effective. I take it you do not associate yourself with that kind of practice?

MR. BUSCH: What is the corroboration practice in New York?

PROFESSOR BLAKEY: They require corroboration.

MR. BUSCH: They do?

PROFESSOR BLAKEY: Yes.

MR. BUSCH: Where do they get the corroboration?

PROFESSOR BLAKEY: They do collateral investigation.

MR. BUSCH: What kind of corroboration is required in New York? Independent of the accomplice? You have to connect it?

PROFESSOR BLAKEY: Yes.

MR. BUSCH: And they make deals like that? I'd say get wiretapping and then we will corroborate them.

PROFESSOR BLAKEY: I am not arguing that you cannot do it with wiretapping; but I am trying

to find out if there is a legal inhibition on your doing it in California, and frankly I have yet to hear what the legal inhibition is. I hear a policy inhibition.

MR. BUSCH: Our grand juries are not really set up on the basis of being investigative bodies.

PROFESSOR BLAKEY: Is that legally or traditionally?

MR. BUSCH: It is traditional and I think it gets into the legal field, that they are more restricted in what they can do than other types of investigative grand juries.

PROFESSOR BLAKEY: I don't want to belabor the point, Mr. Busch, but I certainly want the record to indicate that I, at least, have not really understood why legally you can't do it.

Let me press you a little bit, if I might—

MR. BUSCH: I don't know if I made it clear to you or not.

PROFESSOR BLAKEY: Let me press you a little bit on the *Jones* case.

What would you do if, as the chief law enforcement officer in the Los Angeles office, the SAC called you and said, "I have a gambling tap in and I just heard there was an assassination plot out on a prominent figure in Los Angeles. Can you see to it that he is given protection and the assassination is prevented?"

MR. BUSCH: We would give it.

PROFESSOR BLAKEY: Wouldn't that be in violation of your California law under the *Jones* case?

MR. BUSCH: No, it wouldn't.

PROFESSOR BLAKEY: If you can't take legal wiretapping evidence from the Federal people—

MR. BUSCH: Oh, no—in the courtroom, sir. *Jones* said we couldn't use it in the court.

PROFESSOR BLAKEY: You can investigate with it?

MR. BUSCH: I don't see why not.

PROFESSOR BLAKEY: And you can respond to it?

MR. BUSCH: I would hope so.

PROFESSOR BLAKEY: But you can't use it in court?

MR. BUSCH: Evidentiary, that is right.

PROFESSOR BLAKEY: As a practical matter now I am thinking of the motivation of policemen. Are policemen disinclined to cooperate with Federal authorities if they think it is legally, now, a one-way street? You can give information to the Federal authorities but you can't get information from them to use in court?

Isn't that the effect of the *Jones* case?

MR. BUSCH: Well, yes. That would be one of the effects of the *Jones* case. But I don't think that

should impede local authorities from cooperating with Federal authorities in the exchange of information.

PROFESSOR BLAKEY: Does it?

MR. BUSCH: No, in our area it does not, as a practical matter. No, it does not.

PROFESSOR BLAKEY: Do your people—

MR. BUSCH: We have a regular network of cooperation.

PROFESSOR BLAKEY: Do your people assist the Federal people in any wiretaps, Federal wiretaps, doing collateral surveillance?

MR. BUSCH: No. When the Task Force goes into any areas that involve wiretapping, we are not involved in it.

PROFESSOR BLAKEY: Why not?

MR. BUSCH: We are not invited along.

PROFESSOR BLAKEY: Do you know why you are not invited along?

MR. BUSCH: Because it is a Federal case.

PROFESSOR BLAKEY: The testimony before this Commission indicates in most other areas of the country when wiretaps are put in, they are really joint efforts; that there are Federal people involved and there are state people involved and there are local people involved, and very often the Federal people get the probable cause and actually man the tap, but a great deal of collateral investigation, identifying people, surveillance, etc. is done by state people.

MR. BUSCH: If they ask us, we will do it.

PROFESSOR BLAKEY: But you are never asked?

MR. BUSCH: Not that I know of.

PROFESSOR BLAKEY: Would you be in a position to know?

MR. BUSCH: Well, I don't know of our men—I will have to just speak for my Bureau of Investigation. Actually, if there is going to be surveillance in the surveillance area of a wiretap calling in and asking us to help—I don't know of any. We will do it if they ask us. I am not familiar that they do it with our large police departments, either.

PROFESSOR BLAKEY: Making an over-all assessment of your own office's response to organized crime and all its areas of activity, do you think you are holding the line, being inundated by it, reversing the problem?

MR. BUSCH: I think it is getting worse in our area. There are a number of factors—increase of pornography, making pornographic films, laundering money—that type of thing. I think it is worse.

PROFESSOR BLAKEY: Do you attribute this in any measure to the existing criminal justice system in California?

MR. BUSCH: I think the lack of some of the tools that are available in other jurisdictions make us a little more attractive.

PROFESSOR BLAKEY: I take it the implication of that answer is if you had wiretapping—

MR. BUSCH: We would do better.

PROFESSOR BLAKEY: You could make a better response to it.

MR. BUSCH: We would.

PROFESSOR BLAKEY: And you have made this kind of testimony available to the State Legislature?

MR. BUSCH: Yes, absolutely.

PROFESSOR BLAKEY: And they have still said no?

MR. BUSCH: They have said no, so far.

PROFESSOR BLAKEY: Thank you very much. I appreciate your candor.

MR. REMINGTON: Judge Shientag.

MS. SHIENTAG: Briefly, Mr. Busch, on consensual wiretapping to which you alluded, when the agent goes in with a body recorder or some such equipment, do you very often have defenses of entrapment posed by the defense?

MR. BUSCH: Yes, ma'am. Whenever we are confronted with the use of consensual—as I say, the best thing is here you are on the telephone because you get such good reception. The other types, the Fargo body recorders require a good deal of contact and the ability to record off them. Generally there will be a quarrel that there was instigation on the part of the agent that was involved, and that he instigated the proposition that was in his mind, et cetera. So there is that defense offered.

MS. SHIENTAG: How do you guard against that defense?

MR. BUSCH: Try to get a very good tape recorder.

MS. SHIENTAG: The instrument, itself?

MR. BUSCH: The instrument, itself, and its ability to record is the best way to overcome that.

MS. SHIENTAG: One of the reasons advanced to us for consensual recordings or body recordings is the agent's life may be in danger were he not overheard by the monitoring group who can move in quickly. Now, that doesn't apply in telephone recordings?

MR. BUSCH: No. If you are going to send an undercover officer in to buy a couple of kilos of heroin, I doubt if that officer is going to take a wire device in with him. That is head-on stuff. If you get caught with a wire recorder, you're dead. So in that type of situation you probably wouldn't have a recorder. You would just have personal surveillance.

If you are talking about somebody going in and bribing a public official and he is not a police of-

ficer, you could wire him up pretty easily without a threat of safety.

The safety factor to me—it probably is involved in some areas but I don't think it would be an important one.

But on the telephone, as I say, and the ability there to get good recordings, there is no safety factor involved at all.

MS. SHIENTAG: But there could be a possible defense of entrapment that would be valid?

MR. BUSCH: Oh, yes, ma'am.

MS. SHIENTAG: Because you are enticing this man to make statements to you?

MR. BUSCH: That is absolutely true.

MS. SHIENTAG: And using him as a come-on for the defendant?

MR. BUSCH: One of the considerations you have to take into account is that the person does not become the aggressor of the conversations. If it is going to be a good investigation you let the suspect do the talking.

MS. SHIENTAG: One question on your statement that you haven't been able to sell it to the Legislature yet—

MR. BUSCH: Yes.

MS. SHIENTAG: —that is, court-ordered wire-tapping.

MR. BUSCH: Yes.

MS. SHIENTAG: What have some of the recent attempts been since 1968?

MR. BUSCH: We do it every year.

MS. SHIENTAG: Is it the District Attorneys Association?

MR. BUSCH: Yes, ma'am. I am president of the California District Attorneys Association. We have offered the bill. The California Attorney General has offered the bill.

I can say very frankly that we have a tough committee in our State Legislature with reference to any law-enforcement-oriented bills.

MS. SHIENTAG: Well, what is needed to get it through the Legislature?

MR. BUSCH: Well, it has to come out of committee, the Criminal Justice Committee, and we can't get it out of committee. That is our problem.

MS. SHIENTAG: Is your governor interested in the subject?

MR. BUSCH: Our past governor was. Our present governor—I have not talked with him about it.

MS. SHIENTAG: You know that his father had been interested and has sponsored wiretapping?

MR. BUSCH: Yes, ma'am, but the young Mr. Brown is an entirely different personality than his father.

MS. SHIENTAG: In your considered judgment, what is the possibility of having court-ordered wire-tapping out there?

MR. BUSCH: I think as we accumulate the instances, such as the union officials, the various ones that I have talked about where, as I say—to me, to just give immunity, transactional immunity to everybody in a prosecution is a poor prosecutorial weapon. And I think when we gather enough evidence to show what is happening and what we are lacking, we will be able to convince the Legislature. I honestly believe that.

MS. SHIENTAG: And you think the evidence from other jurisdictions and the Federal Government might persuade them?

MR. BUSCH: Oh, yes, certainly. And the best one I have ever seen, as I say, came out of Kings County. When they see what they can do with it we will be able to sell it—with the safeguards.

I understand the feelings about people and about Big Brother watching and listening, but you have to have some confidence in Big Brother once in a while, I think.

MS. SHIENTAG: Thank you, Mr. Busch.

Thank you, Mr. Chairman.

MR. REMINGTON: Chief Andersen.

CHIEF ANDERSEN: Mr. Busch, in your opposition in the Legislature is it mostly from northern or southern California or is there any geographical difference?

MR. BUSCH: No, there is no geographical fight about it. It is a philosophical fight, the extension of the power of the court, through court order, to listen in on conversations where people are unaware that they are being listened to.

CHIEF ANDERSEN: So it is not southern California?

MR. BUSCH: No, it isn't a territorial fight.

CHIEF ANDERSEN: Does your Attorney General have independent investigative powers in California—I mean a statewide grand jury? Do you have that concept in California?

MR. BUSCH: No, he can move into any county he wants to if there has been a break-down in law enforcement.

CHIEF ANDERSEN: But he doesn't as a practical fact?

MR. BUSCH: No. There is a Department of Justice. It does have a Narcotics Division and they do have investigative units. They usually turn their matters over to the local District Attorney.

CHIEF ANDERSEN: On illegal wiretapping, have you had any state prosecutions for this in Los Angeles County?

MR. BUSCH: Yes. From time to time we run across private detectives who are tapping in and

listening. I have not seen a prosecution of a public agency of illegal wiretapping—but of private individuals, I have.

CHIEF ANDERSEN: With private individuals you have had prosecutions in this area?

MR. BUSCH: Absolutely.

CHIEF ANDERSEN: On your consensual recordings, I got the impression that all of it is handled from your office, the District Attorney's Office. Is it all handled from your office?

MR. BUSCH: No.

CHIEF ANDERSEN: Are your police divisions independent in this area?

MR. BUSCH: Yes. The major police departments have the ability to do consensual tapping. We have 55 police departments in our county and some of the smaller ones, of course, wouldn't be equipped for it so they call upon the Sheriff for their aid. And generally speaking, in that kind of case, where there is a consensual, we have lawyers in on it right from the start.

CHIEF ANDERSEN: But they use this independently as an investigative tool and it is not a prosecutorial tool only?

MR. BUSCH: Yes. If there was a local kidnapping, there would be immediate initiative to handle that on their own.

CHIEF ANDERSEN: On your *Jones* decision, have you had any problems in cooperation with other states on this? I know we have talked about Federal wiretapping, but have you had acquaintance with another state's wiretapping evidence being involved in your county?

MR. BUSCH: I am unaware of any.

CHIEF ANDERSEN: It just hasn't come up?

MR. BUSCH: No, but we will exchange information. We will be exchanging information with New York or Philadelphia or Chicago. If that information is coming from non-consensual wiretaps from New York, we wouldn't know of that; but we would cooperate—unless they told us it was as a result of a tap.

CHIEF ANDERSEN: So the problem just hasn't arisen?

MR. BUSCH: It has not arisen.

CHIEF ANDERSEN: That is all, Mr. Chairman. Thank you, Mr. Busch.

MR. REMINGTON: Mr. Busch, on page 9 of your statement you state that the proposed legislation is highly restrictive and that it actually begins where the Federal Government leaves off in terms of restrictions.

Generally, what restrictions are imposed in California that are not part of the Federal legislation?

MR. BUSCH: In general, our legislation was not for as extensive a period of time as the Federal law was, and it would require monitoring by the judge and it would require you to bring in certain aspects of it. Also, in the monitoring, there is the requirement that it not be a constant monitoring, that if it was obvious that the conversation did not further the investigation pursuant to the court order, it not be made part of the permanent record—and that type of thing.

In other words, there would be editing of it somewhat. Whether that is good or bad, it is an endeavor to do some of those things.

MR. REMINGTON: In your judgment, are those further restrictions important to have on their merits, or do you feel that was necessary in order to get the legislation adopted?

MR. BUSCH: On the merits? Well, it just seems to me it answers some of the problems we are confronted with as an invasion of privacy. Yes, on the merits and as an answer to some of the criticisms that are made with reference to constant eavesdropping.

MR. REMINGTON: I take it it would be your view that this Commission in reviewing Federal legislation ought to take note of the further proposals in California and give consideration as to whether those might not be appropriate, and changes made in Federal legislation?

MR. BUSCH: Yes.

PROFESSOR BLAKEY: Mr. Chairman, I wonder if we could have the staff get a copy of the proposed bill?

MR. BUSCH: I would be glad to send it, surely.

PROFESSOR BLAKEY: And if it could be appended somewhere to your testimony in the record.

MR. BUSCH: Sure, I would be glad to do that.

[The proposed bill in the California Legislature follows.]

SENATE BILL No. 668

Introduced by Senator Biddle

April 10, 1973

An act to add Chapter 3.5 (commencing with Section 1544.1) to Title 12 of Part 2 of the Penal Code, relating to collection of nonphysical evidence.

LEGISLATIVE COUNSEL'S DIGEST

SB 668, as introduced, Biddle. Collection of nonphysical evidence.

Authorizes issuance by court of appeal or superior court, on application of Attorney General or district attorney, of order authorizing interception of wire and oral communication by electronic, mechanical, or other device, as defined. Prescribes form and content of application for order and of order, conditions for issuance of order, period of effectiveness, procedure for renewal, time and procedure for return, notice to the person named in the order, and records to be maintained with regard to

order. Authorizes prescribed disclosures and uses of information obtained pursuant to such provisions with respect to official duties or testimony in criminal court proceeding or grand jury proceeding. Prescribes civil liability of persons who eavesdrop in unauthorized manner or make improper disclosure.

Provides that neither appropriation is made nor obligation created for the reimbursement of any local agency for any costs incurred by it pursuant to the act.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: no state funding.

The people of the State of California do enact as follows:

Section 1. Chapter 3.5 (commencing with Section 1544.1) is added to Title 12 of Part 2 of the Penal Code, to read:

CHAPTER 3.5 ELECTRONIC EVIDENCE COLLECTION

1544.1. This chapter shall be known and may be cited as the "Electronic Evidence Collection Act of 1973."

1544.2. The Legislature hereby declares the following to be statements of legislative intent:

(a) The Legislature intends that this chapter shall implement subdivision 2 of Section 2516 of Title 18 of the United States Code.

(b) The Legislature intends that every act which complies with the provisions of this chapter shall also comply with Section 2518 of Title 18 of the United States Code.

1544.3. As used in this chapter:

(a) "Wire communication" means any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other connection between the point of origin and the point of reception.

(b) "Oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation.

(c) "Intercept" means the acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device.

(d) "Electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire or oral communication, except:

(1) Any telephone or telegraph instrument, equipment or facility, or any component thereof, either (i) furnished to the subscriber or user by a of its business and being used by the subscriber or user in the ordinary course of its business, or (ii) being used by a communications common carrier in the ordinary course of its business or by a peace officer in the ordinary course of his duties.

(2) A hearing aid or similar device being used to correct subnormal hearing to not better than normal.

(e) "Communications common carrier" means any public utility engaged in the business of providing wire or radio communications services and facilities.

(f) "Judge" means any judge of a court of appeal or judge of the superior court of the county in which the order is to be executed or of the county in which an office of the applicant is located.

(g) "Aggrieved person" means a person who was a party to an intercepted wire or oral communication, a person against whom the interception was directed, or a person on whose premises the intercepted communication occurred.

(h) "Offense" means murder, kidnapping, robbery, bribery, extortion, a felony violation of a law of this state involving theft or dealing in narcotics or restricted dangerous drugs, bookmaking as prohibited by Section 337a, or transmitting racing information to gamblers as prohibited by Section 337i, or conspiracy to commit any of the foregoing.

(i) "Contents," when used with respect to any wire or oral communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.

1544.4. Each application for an order authorizing the interception of a wire or oral communication shall be made in writing upon the personal oath or affirmation of the Attorney General or of a district attorney to a judge. Each application shall include all of the following information:

(a) The identity of the investigative or law enforcement officer making the application, and the officer authorizing the application.

(b) The identity of the law enforcement agency which is to execute the order.

(c) A full and complete statement of the facts and circumstances relied upon by the applicant to justify his belief that an order should be issued, including (1) details as to the particular offense that has been, is being, or is about to be committed, (2) a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (3) a particular description of the type of communications sought to be intercepted, and (4) the identity, if known, of the person committing the offense and whose communications are to be intercepted, or if such identity is not known, then such information relating to the person's identity as is known to the applicant.

(d) A full and complete statement as to whether other investigative procedures have been tried and failed, or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous.

(e) A statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter.

(f) A full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge of a state or federal court for authorization to intercept wire or oral communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application.

(g) Where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

1544.5. Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing interception of wire or oral communications within the territorial jurisdiction of the court in which the judge is sitting, if the judge determines on the basis of the facts submitted by the applicant all of the following:

(a) There is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense.

(b) There is probable cause for belief that particular communications concerning that offense will be obtained through such interception.

(c) Normal investigative procedures have been tried and have failed or reasonably appear to be either unlikely to succeed if tried or to be too dangerous.

(d) There is probable cause for belief that the facilities from which, or the place where, the wire or oral communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

1544.6. Each order authorizing the interception of any wire or oral communication shall specify:

(a) The identify, if known, of the person whose communications are to be intercepted, or if such identity is not known, then such information relating to the person's identity as is known to the applicant.

(b) The nature and location of the communications facilities as to which, or the place where, authority to intercept is granted.

(c) A particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates.

(d) The identity of the agency authorized to intercept the communications, and of the person making the application.

(e) The period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

1544.7. No order entered under this chapter may authorize the interception of any wire or oral communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than 10 days. Extensions of an order may be granted, but only upon application for an extension made in accordance with Section 1544.4 and upon the court making the findings required by Section 1544.5. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than 10 days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in 10 days.

1544.8. An order authorizing interception, entered pursuant to this chapter, may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

1544.9. The contents of any wire or oral communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire or oral communication pursuant to this chapter shall be done in such a way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for 10 years. Duplicate recordings may be made for use or disclosure, pursuant to the provisions of Sections 1544.14 and 1544.15, for investigations. The presence of the seal provided for by this section, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire or oral communication or evidence derived therefrom under Section 1544.16.

1544.10. Applications made and orders granted pursuant to this chapter shall be sealed by the judge. Custody of the applications and order shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for 10 years.

1544.11. Within a reasonable time, but not later than 30 days, after the termination of the period of an order or extensions thereof, the issuing judge shall cause to be served, on the persons named in the order or the application, and other known parties to intercepted communications an inventory which shall include notice of all of the following:

(a) The fact of the entry of the order.

(b) The date of the entry and the period of authorized interception.

(c) The fact that during the period wire or oral communications were or were not intercepted

The judge, upon the filing of a motion, may, in his discretion, make available to such person or his counsel for inspection such portions of the intercepted communications, applications, and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge, the serving of the inventory required by this section may be postponed. The period of postponement shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than 30 days for each such showing.

1544.12. The contents of any intercepted wire or oral communication or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding, except a grand jury proceeding, unless each party, not less than 10 days before the trial, hearing, or proceeding, has been furnished with a transcript of the contents of such interception and with a copy of the court order, and accompanying application, under which the interception was authorized. This 10-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information 10 days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

1544.13. Any aggrieved person in any trial, hearing, or proceeding may move to suppress some or all of the contents of any intercepted wire or oral communication, or evidence derived therefrom, on any of the following grounds:

(a) The communication was unlawfully intercepted.

(b) The order of authorization under which it was intercepted is insufficient on its face.

(c) The interception was not made in conformity with the order of authorization.

(d) The communication, or some portion thereof, is not directly relevant to proving the offense charged.

Such motion shall be made and determined pursuant to the provisions of Section 1538.5.

1544.14. The Attorney General or any deputy attorney general, district attorney or deputy district attorney, or any peace officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire or oral communication, or evidence derived therefrom, may disclose such contents to one of the individuals referred to in this section to the extent that such disclosure is appropriate to the proper performance of the official duties of the individual making or receiving the disclosure.

1544.15. The Attorney General or any deputy attorney general, district attorney or deputy district attorney, or any peace officer, who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire or oral communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.

1544.16. Any person who has received, by any means authorized by this chapter, any information concerning a wire or oral communication, or evidence derived therefrom, intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any criminal court proceeding or in any grand jury proceeding.

1544.17. No otherwise privileged wire or oral communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character

1544.18. When a peace officer, while engaged in intercepting wire or oral communications in the manner authorized by this chapter, intercepts wire or oral communications relating to crimes other than those specified in the order of authorization,

the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in Section 1544.14 and 1544.15. Such contents and any evidence derived therefrom may be used under Section 1544.16 when authorized by a judge where such judge finds on subsequent application, that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

1544.19. Any violation of the provisions of Sections 1544.9, 1544.10, and 1544.11 shall be punished as contempt of court.

1544.20. (a) Any aggrieved person who has been injured by a violation of this chapter may bring an action against the person who committed the violation for the greater of either three thousand dollars (\$3,000) or three times the amount of actual monetary damages, if any, sustained by the plaintiff.

(b) Any aggrieved person may, in accordance with the provisions of Chapter 3 (commencing with Section 525) of Title 7 of Part 2 of the Code of Civil Procedure, bring an action to enjoin and restrain any violation of this chapter, and may in the same action seek damages as provided in subdivision (a).

(c) It is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual monetary damages.

A good faith reliance on a court order, or on any other legislative authorization, shall constitute a complete defense to any civil or criminal action brought under this chapter, or under Chapter 1.5 (commencing with Section 630) of Title 15 of Part 1, or any other law.

1544.21. Nothing in Section 631 or 632 shall be construed as prohibiting any peace officer from intercepting any wire or oral communication pursuant to an order issued in accordance with the provisions of this chapter. Nothing in Section 631 or 632 shall be construed as rendering inadmissible in any criminal proceeding in any court or before any grand jury any evidence obtained by means of an order issued in accordance with the provisions of this chapter. Nothing in Section 637 shall be construed as prohibiting the disclosure of the contents of any oral or wire communication obtained by any means authorized by this chapter, if such disclosure is authorized by this chapter.

1544.22. Notwithstanding any other provision of law, any court to which an application is made in accordance with this chapter may take any evidence, make any finding, or issue any order required to conform the proceedings or the issuance of any order of authorization or approval to the provisions of the Constitution of the United States or of any law of the United States.

1544.23. If any provision of this chapter, or the application thereof to any person or circumstances, is held invalid the remainder of the chapter, and the application of its provisions to other persons or circumstances, shall not be affected thereby.

Sec. 2. No appropriation is made by this act, nor is any obligation created thereby under Section 2164.3 of the Revenue and Taxation Code, for the reimbursement of any local agency for any costs that may be incurred by it in carrying on any program or performing any service required to be carried on or performed by it by this act.

MR. REMINGTON: One of the matters on which we get conflicting opinions expressed is the matter of how important the problem is that we are dealing with, that is, the problem of criminal activity that might be dealt with effectively by that kind of surveillance.

On the one hand, we have people saying that the problems are not very important, that if there is to be electronic surveillance it ought to be limited to

murder, kidnaping, espionage. And, on the other hand, we have people who express the view that the problem of what is referred to as organized crime is an immensely serious problem that we need to give attention to and deal with in a more effective way than we have in the past.

In your view, how important is the issue? Is it, for example, confined to murder, kidnaping, and espionage, or rather other aspects of the problem of organized crime, if that is what it is, that we need to be concerned about?

MR. BUSCH: To make a laundry list of particular crimes I think is a difficult thing, because it all depends on what impact you are having on your environment, on your community, with reference to what kind of criminal activity is going on. And to limit it to a particular laundry list, I don't think is too appropriate, although I think it is necessary to do it in order to get that kind of legislation through.

The important thing about it, I believe, is that it is a tool that should be made available to law enforcement on a legitimate basis, because it is a loophole for criminals to get around and communicate in their activities. And when we talk about this—and the thing that I think is so important—it is up to the investigating agency to convince the magistrate, convince the judge, that they have exhausted all the other means that they could have possibly used in arriving at a solution to the problem that is facing their environmental or their local areas in that area.

And I think that is the important thing. As long as you have exhausted surveillance—and I don't like the immunity bit too much, Mr. Blakey. It is a tool, but it is a tool—that is a tool—I don't like to see guys walking away all the time.

So if the agency can establish for the judge that they have exhausted everything and this is what they want to do, and they confine the area, and the court is the watchdog of it, and there is proper recording and proper keeping of these things, I think it is a valuable tool.

MR. REMINGTON: From your experience in Los Angeles, if someone were to say with regard to this, "What kind of targets do you have in mind when you say this is needed?"—with regard to what kind of things that are happening in Los Angeles do you feel you have particular need for authority to conduct non-consensual surveillance?

MR. BUSCH: I would really like to see it in the narcotic area. I would really like to see it in that particular area.

And I do think that in kidnappings and in murders for hire and that type of thing, it should be readily available—extortions—those general areas.

The reason I say that, and particularly governmental corruption—is those are the areas where you have the most difficult time not utilizing the other means of solving crime. Those are the areas where you run up against a stone wall and are stopped.

If it meant naming a laundry list to have electronic surveillance, then I think it would be appropriate to name a list and we would do that.

MR. REMINGTON: Are there other questions?

PROFESSOR BLAKEY: Mr. Busch, let me ask you at least two additional questions.

In the Federal system, under a memorandum promulgated by former Attorney General Clark, all consensuals, except in exigent circumstances, have to have prior prosecutive approval. This is also the law in Illinois. Recently, too, the American Bar Association promulgated an ethical opinion dealing with the participation of attorneys in consensuals.

I wonder if you could share with us your own opinion of restricting police use of this technique to situations where there is some responsible participation by prosecuting authorities?

MR. BUSCH: I have no quarrel with that. I think in those kinds of cases it is probably better to have a lawyer there, really.

PROFESSOR BLAKEY: Do you think your people could be geared up enough to supervise the police and other law enforcement agencies in the community?

MR. BUSCH: Yes.

PROFESSOR BLAKEY: So they couldn't do it unless they got your permission?

MR. BUSCH: Yes. As a matter of fact, I would prefer it that way if they are going to go into the consensual area because I think a lawyer should be there from the outset.

When you put a policy like that into effect, what does it mean if they just snatched a little kid and they wanted to listen in to the ransom call and the District Attorney wasn't there yet and they went ahead—you can always think of horror stories that have to be exceptions.

But, outside of the horror stories that would be exceptions, I would say yes, it would be most appropriate.

PROFESSOR BLAKEY: Do you have a legal unit that works with the Los Angeles Police Department?

MR. BUSCH: Other than for educational purposes—

PROFESSOR BLAKEY: When they ask for search warrants currently, do they get your approval?

MR. BUSCH: Yes, search warrants are issued by my office.

PROFESSOR BLAKEY: So they don't go to a magistrate on their own-direct?

MR. BUSCH: No, sir.

PROFESSOR BLAKEY: Do you have any other continuing day-to-day operation where you can give them legal advice in investigations?

MR. BUSCH: Yes. We are a factory—

PROFESSOR BLAKEY: I am familiar with your office.

MR. BUSCH: So our Complaint Division is always available for advice and consultation with the officers.

PROFESSOR BLAKEY: Let me press you a little more on this aspect of it.

Testimony before the Commission indicates that in a number of other areas there are police-prosecutor units. In the Federal system, they call them Strike Forces; in New York City, Racket Bureaus. In other places, they have other names. But the philosophy behind them is that in certain sophisticated kinds of investigations—not only in organized crime but also, for example,—there is a need early on for legal participation in the investigatory process.

Do you have any comparable policy and practice in Los Angeles?

MR. BUSCH: Only in the organized crime-narcotics—when I say “narcotics” I mean organized narcotics activity—and the Special Investigations Unit.

But we always have help available for the police departments. Whenever they want help at the investigative stage, we will assign people to it. But I don't create task force units. In other words, I don't have a homicide unit and a robbery unit.

PROFESSOR BLAKEY: In other words, you don't have lawyer participation in the investigation unless the police want it?

MR. BUSCH: That is right.

PROFESSOR BLAKEY: Do they want it?

MR. BUSCH: Oh, they call for it frequently, yes.

PROFESSOR BLAKEY: Is your Intelligence Unit a member of LEIU?

MR. BUSCH: Yes, I believe it is.

PROFESSOR BLAKEY: Do you know whether LEIU accepts intelligence data based on wiretaps?

MR. BUSCH: I would think they did.

PROFESSOR BLAKEY: If they do, how can you use it in light of *Jones*?

MR. BUSCH: We couldn't use it in the courtroom.

PROFESSOR BLAKEY: But you would use it for background?

MR. BUSCH: You could use it for investigation and knowledge.

PROFESSOR BLAKEY: How would you disentangle it?

MR. BUSCH: As I say, I don't know how far the *Jones* case is going to go, because that was even a legal wiretap.

PROFESSOR BLAKEY: I know.

MR. BUSCH: And I just don't know how far they will go. But it was the use of the wiretap, itself, that the *Jones* case was involved in.

Now, if they are going to say we can't do it, then we have problems.

PROFESSOR BLAKEY: The Law Enforcement Intelligence Unit is, for the record, a multi-state, multi-departmental cooperative program with intelligence units where people share information about leading figures and attempt to keep people abreast of their own crime problems.

If units which feed into that pool have intelligence that is based on wiretapping, I take it the common pool would be polluted under the most liberal use of *Jones*?

MR. BUSCH: Yes, it would be.

PROFESSOR BLAKEY: And you could possibly bring a motion to suppress on the grounds that this was based on something out of LEIU that was based on a wiretap in New York?

MR. BUSCH: I assume they will do that. I hope that is not what the *Jones* case means.

PROFESSOR BLAKEY: Would that have a substantial disruptive effect on your prosecutions?

MR. BUSCH: Yes, it would.

PROFESSOR BLAKEY: Could you afford to stay in the LEIU if that would be the impact of it?

MR. BUSCH: I can't answer that. I don't know the impact of it. We have to wait.

PROFESSOR BLAKEY: Or, conversely, can those people whose intelligence programs depend in major part on wiretap information afford to stay in LEIU if their compatriots could not share their wiretap information?

MR. BUSCH: You know, it is a real can of worms because we are not talking about just any intelligence unit, but about all of California's.

PROFESSOR BLAKEY: It seems as if California has to sort of secede from the nation in organized crime programs.

MR. BUSCH: I really don't think that is what they intend by the *Jones* case.

PROFESSOR BLAKEY: If you were a defense counsel, how far would you take it?

MR. BUSCH: All the way.

PROFESSOR BLAKEY: Do you have any reason to think that the California bar won't?

MR. BUSCH: No.

PROFESSOR BLAKEY: Do you have any reason to believe, in reading the *Jones* opinion, itself, that the court that rendered that decision won't take it all the way?

MR. BUSCH: Yes—well, as I say, I think if confronted with the particular situation that you are speaking of, they might reassess their opinion.

PROFESSOR BLAKEY: Do you think it would be helpful if Federal legislation changed the *Jones* decision?

MR. BUSCH: Well, if it would solve these problems that you are talking about, yes. But I don't know whether that is possible. You know, can Federal legislation overrule the California Supreme Court?

PROFESSOR BLAKEY: It is pretty clear it can constitutionally. The question is whether it would be the wisest policy. If you are only talking about the administration of California's courts, that is California's problem. But if that rule began to have an impact on other states—and it might through LEIU—or if that rule began to have an impact on Federal-state cooperation in California and it began to impede Federal narcotics investigations because people in California were reluctant to cooperate because it was not a two-way street, it seems to me something could be done by Congress saying that lawful Federal wiretap evidence is admissible in Federal or state proceedings. They have now said an unlawful tap is inadmissible in federal or state proceedings. Why can't they do the reverse?

MR. BUSCH: I will talk to a couple of my Congressmen and see if they won't address themselves to the problem.

PROFESSOR BLAKEY: Thank you.

MR. BUSCH: Thank you, sir.

MR. REMINGTON: Mr. Busch, I have one final question, but I will defer that for a moment. General Hodson.

MR. HODSON: Mr. Busch, I know you are very proud of your office. We have been using a questionnaire in other prosecutive offices. The questionnaire indicates the average salaries, number of personnel, case load, work load, and so forth.

I would like to request that you fill out such a questionnaire for us and that it be made a part of the record.

MR. BUSCH: I would be very glad to. The Administrator of our office just negotiated a new contract with the county and they got themselves quite a substantial raise.

MR. HODSON: Thank you.

MR. REMINGTON: Mr. Busch, I would like to ask a very general, and probably difficult to answer, but I think, nonetheless, important question.

You made reference to this earlier in your testimony.

In my observation, there is a very different attitude here in Washington, for example, between

concern over electronic surveillance on the one hand and concern over who is arrested or who is subject to a physical search on the other hand. I think it is a valid generalization to say, for example, Congress has been very concerned about electronic surveillance and has been equally unconcerned about who gets arrested, whether there has to be judicial authority to make an arrest, who gets searched and whether there has to be judicial authority to conduct a physical search.

In your view, based on your lengthy experience in law enforcement, why that difference?

MR. BUSCH: Well, you know, from a political standpoint, I suppose the hotter issue is the invasion of privacy nowadays rather than who is getting arrested and what the basis for the arrest is.

It is my personal feeling, that it is a hotter political issue.

The laws of arrest, of course—I am only familiar with our own in California, and just through Appellate decisions we have pretty well estopped frisk situations. It is well outlined, when you can stop and frisk and what amounts to an arrest and what doesn't amount to being taken into custody and what is reasonable and probable cause for arrest.

So that has not really been a matter of great concern in our Legislature.

When you speak of it, are you talking about Washington, D.C. or Federal law generally?

MR. REMINGTON: I think probably legislatures in general.

For example, in California is it lawful to make an arrest without a warrant in circumstances where it would have been possible to get a warrant?

MR. BUSCH: Yes.

MR. REMINGTON: So, in other words, it is possible in California, as it is in the Federal system, to take a person into custody without prior judicial approval, even though it would have been possible to get prior judicial approval?

MR. BUSCH: Yes.

MR. REMINGTON: I might say parenthetically, if I were given a choice to be listened to or arrested, I would rather be listened to.

MR. BUSCH: I'm sorry, I misunderstood. I thought you meant why were they addressing themselves—

MR. REMINGTON: The question is: Why is there a national commission on listening, why are several committees looking into it, why are several legislatures concerned, and at the same time there is almost total absence of concern with who is arrested or, as you indicated in your testimony, who is subject to physical search?

That is not intended to be a leading question. I have difficulty answering the question, myself.

What is it about this field that gets people, particularly those who hold political office, so excited when they seem so unexcited about other issues of the kind?

MR. BUSCH: Well, maybe it is because they feel that governmental corruption—politicians, themselves, are going to be listened to by wiretap, if they have a wiretap law, under court order.

MR. REMINGTON: Do you think it is largely a question of economics, that by and large poor people get arrested, and by and large wealthy people get listened to?

MR. BUSCH: I would say that would be a fair statement, that most people who are arrested are poor people and most people you are going to be listened to are going to be people of some substance.

MR. REMINGTON: Are there any other questions?

[No response.]

Mr. Busch, we are very appreciative of your willingness to be here this morning. Your testimony has been extremely helpful to us and we very much appreciate your coming out from Los Angeles to be with us.

MR. BUSCH: I appreciate being here. I hope I have been of help to you. I hope I haven't been too confusing about our grand jury system, but it has been a pleasure to be here.

Thank you very much.

MR. REMINGTON: You have been very helpful. We appreciate it.

I think we will take a short five-to-ten minute recess at this point.

[Whereupon, a short recess was taken.]

MR. REMINGTON: I think we will try to resume, if we may.

We turn our attention next to the City of Chicago, Cook County.

We have heard from Mr. James Thompson that he is tied up this morning, but will be here with us later and we will look forward to hearing from him this morning.

In the meantime, we welcome Mr. Kenneth Gillis, who is head of the Special Prosecutions Bureau, and Mr. Nicholas Iavarone of the Organized Crime and Corruption Task Force of the States Attorney's Office in Chicago.

I understand both have been involved in the past year in a major investigation of an organized theft ring, and based on their experience and other experiences in prosecution work, we look forward to the opportunity to hear from them as to the method of investigation which they have been able to use in Cook County, their views as to whether they would be able to be more effective in their work if they

were able under their law to employ non-consensual electronic surveillance work.

In the State of Illinois consensual electronic surveillance requires the request of the State's Attorney, and I assume we will hear whether that works well or creates practical problems.

So we welcome both of you here this morning and certainly appreciate your coming out from Chicago to meet with us and look forward to hearing from you.

But, first, under the rules of the Commission I will have to swear you.

[Whereupon, Kenneth Gillis and Nicholas Iavarone were duly sworn by the Chairman pro tem.]

**TESTIMONY OF KENNETH GILLIS,
DEPUTY STATE'S ATTORNEY,
SPECIAL PROSECUTIONS BUREAU;
AND NICHOLAS IAVARONE,
ORGANIZED CRIME AND
CORRUPTION TASK FORCE, COOK
COUNTY, ILLINOIS**

MR. REMINGTON: I presume, Mr. Gillis, that you want to start. You may proceed in any way you like.

MR. GILLIS: Mr. Remington, it is indeed a pleasure to meet with you and share our ideas and procedures from the State of Illinois with such a distinguished Commission as yourselves.

As I listened to your questions, I can see that you have developed keen expertise in this area. Your questions also indicate a concern and a tone that I think is so necessary in an area where a balance of the powers of law enforcement and the rights of individuals is quite obviously important.

We have, in the State of Illinois, a consensual statute that roughly permits the recording of a conversation with the consent of one of the parties, and also with the prior consent and request of the State's Attorney.

This method of preserving evidence—and I think that seen in its proper light that is what it is, an electronic stylus, if you will, that records oral conversations and makes their presentation into a court of law no longer one of guess-work or one of opinion, but one of higher evidence.

This technique that we have had under our statute has been invaluable to use. It has permitted us to gain convictions of public officials, police officers for bribery, others for extortion. It has been extremely useful in the crime of solicitation to commit murder. We have been able to gather the evidence that is crucial in gaining guilty verdicts and findings in those areas.

It has also been extremely helpful to us in cases where oral evidence is important in proving criminal intent, and often these are cases involving stolen goods; and it is also very helpful in the area of narcotics sales, where the defense of entrapment could easily be put forward if it is one person's word against another, but with the tape recorder there the evidence is made clear as to what exactly transpired.

In Illinois at the present time we have an amendment to our present law—and we have provided staff with a copy of it. It is our House Bill 212. That amends our present law, which I think has been extremely helpful to law enforcement and limits our power under the law. I think, in short, it is a bad bill.

[The text of the bill referred to follows.]

Illinois State's Attorneys Association
211 WEST CHICAGO AVENUE—HINSDALE, ILLINOIS
60521
312/654-1555

ROBERT N. HUTCHISON
EXECUTIVE DIRECTOR
BRENT F. CARLSON
ASSOCIATE DIRECTOR

May 21, 1975

MEMORANDUM

TO: Legislative Committee
FROM: Robert N. Hutchison, Executive Director
RE: H.B. 212-Eavesdropping Consent

The attached bill has passed the House and probably will be scheduled to be heard before the Senate Judiciary Committee within the next week.

Please call Marty Rudman at (815) 729-8453 and express your views on the merits of this legislation. It is extremely important that the Association take an immediate position on this bill if we are to have any influence on its fate in the Senate.

**HOUSE BILL 212
79th GENERAL ASSEMBLY
State of Illinois
1975 and 1976**

INTRODUCED January 23, 1975. BY Representatives Jaffe, Schneider, Denvers, Greiman, Polk, Yourell, Kelly, Berman, Marovitz, Schroeder, K. M. Barnes and Mann. Read first and ordered printed.

SYNOPSIS: (Ch. 38, par. 14-2)

Amends the Criminal Code. Provides that eavesdropping is an offense unless all parties to the conversation have consented thereto

AN ACT to amend Section 14-2 of the "Criminal Code of 1961", approved July 28, 1961, as amended.

Be it enacted by the People of the State of Illinois, represented in the General Assembly:

Section 1. Section 14-2 of the "Criminal Code of 1961", approved July 28, 1961, as amended, is amended to read as follows:

(Ch. 38, par. 14-2)

Sec. 14-2. Elements of the offense. A person commits eavesdropping when he:

(a) Uses an eavesdropping device to hear or record all or any part of any conversation unless he does so with the consent of all of the parties to such conversation and at the request of a State's Attorney; or

(b) Uses or divulges, except in a criminal proceeding, any information which he knows or reasonably should know was obtained through the use of an eavesdropping device.

Adopted April 18, 1975

OFFERED IN JUDICIARY II COMMITTEE BY REP. MANN
Amendment No. 1 Tabled

AMENDMENT TO HOUSE BILL 212

AMENDMENT NO. 2. Amend House Bill 212 on June 2, by deleting period and inserting: "and Article 108 A is added to the 'Code of Criminal Procedure of 1963', approved August 14, 1963, as amended."; and on line 11, between "so" and "with" insert "(1)"; and by deleting line 13 and in lieu thereof inserting "conversation

or (2) with the consent of any one party to such conversation and in accordance with Article 108 A of the "Code of Criminal Procedure of 1963", approved August 14, 1963, as amended; or"; and

By deleting line 14 and in lieu thereof inserting: "Uses or divulges, except

as authorized by Article 108 A of the "Code of Criminal Procedure of 1963", approved August 14, 1963, as amended,"; and

By adding after line 16 the following:

Section 2. Article 108 A is added to the "Code of Criminal Procedure of 1963", approved August 14, 1963, the added Article to read as follows: ARTICLE 108 A. JUDICIAL SUPERVISION OF THE USE OF EAVESDROPPING DEVICES. (Ch. 38, par. 108A-1.)

Section 108A-1. Authorization for Use of Eavesdropping Device. The State's Attorney may authorize an application to a circuit judge for, and such judge may grant in conformity with this Article, an order authorizing or approving the use of an eavesdropping device by a law enforcement officer or agency having the responsibility for the investigation of any felony under Illinois law where any one party to a conversation to be monitored, or previously monitored in the case of an emergency situation as defined in this Article, has consented to such monitoring.

(Ch. 38, par. 108A-2).

Sec. 108A-2. Authorized Disclosure or Use of Information.

(a) Any law enforcement officer who, by any means authorized in this Article, has obtained knowledge of the contents of any conversation overheard or recorded by use of an eavesdropping device or evidence derived therefrom, may disclose such contents to another law enforcement officer or prosecuting attorney to the extent that such disclosure is appropriate to the proper performance of the official duties of the person making or receiving the disclosure.

(b) Any investigative or law enforcement officer who, by any means authorized in this Article, has obtained knowledge of the contents of any conversation overheard or recorded use of an eavesdropping device or evidence derived therefrom, may use the contents to the extent such use is appropriate to the proper performance of his official duties.

(c) Admissibility into evidence in any judicial, administrative, or legislative proceeding shall be as elsewhere described in this Article.

(Ch. 38, par. 108A-3.)

Sec. 108A-3. Procedure for Obtaining Judicial Approval of Use of Eavesdropping Device.

(a) Where any one party to a conversation to occur in the future has consented to the use of an eavesdropping device to overhear or record the conversation, a judge may grant approval to an application to use an eavesdropping device pursuant to the provisions of this section.

Each application for an order authorizing or subsequently approving the use of an eavesdropping device shall be made in writing upon oath or affirmation to a circuit judge and shall state the applicant's authority to make such application. Each application shall include the following:

(1) the identity of the investigative or law enforcement officer making the application and the State's Attorney authorizing the application;

(2) a full and complete statement of the facts and circumstances relied upon by the applicant to justify his belief that an order should be issued including: (a) details as to the particular felony that has been, is being, or is about to be committed, (b) a particular description of the nature and location of the facilities from which or the place where the conversation is to take place or be monitored; (c) a particular description of the type of communication sought to be monitored; (d) the identity of the party to the expected conversation consenting to the use of an eavesdropping device; (e) the identity of the person, if known, committing the offense and whose conversations are to be overheard by the eavesdropping device;

(3) a full and complete statement as to whether or not other investigative procedures have been tried and have failed or why they appear to be unlikely to succeed or are too dangerous to be tried;

(4) a statement of the specific period of time for which the use of the device is required to be maintained or, if the nature of the investigation is such that the authorization for use of the device should not terminate automatically when the described type of communication is overheard or recorded, a particular description of facts establishing probable cause to believe that additional conversations of the same type will occur thereafter;

(5) a full and complete statement of the existence of all previous applications known to the individual making the application which have been made to any judge requesting permission to use an eavesdropping device involving the same persons or circumstances in the present application, and the action taken by the judge on the previous application;

(6) when the application is for an extension of an order, a statement setting forth the results so far obtained from the use of the eavesdropping device or an explanation of the failure to obtain such results.

(b) The judge may request the applicant to furnish additional testimony, witnesses, or evidence in support of the application.

(Ch. 38, par. 108A-4).

Sec. 108A-4. Grounds for Approval or Authorization. The judge may authorize or approve the use of the eavesdropping device where it is found that:

(a) one party to the conversation has or will have consented to the use of the device;

(b) there is probable cause for believing that an individual is committing, has committed, or is about to commit a felony under Illinois law;

(c) there is probable cause for believing that particular conversations concerning that felony offense will be obtained through such use;

(d) normal investigative procedures have been tried and have failed or reasonably appear to be either unlikely to succeed or too dangerous; and

(e) for any extension authorized, that further use of a device is warranted on similar grounds.

(Ch. 38, par. 108A-5)

Sec. 108A-5. Orders Authorizing Use of an Eavesdropping Device.

(a) Each order authorizing or approving the use of an eavesdropping device shall specify:

(1) the identity of the person who has consented to the use of the device to monitor any of his conversations and a requirement that any conversation overheard or received must include this person;

(2) the identity of the other person or persons, if known, who will participate in the conversation;

(3) the place where such conversations are to occur or, if the conversation is not to take place in person, the location of the sources of the conversations, if known;

(4) the times such conversations are expected to occur and be overheard or recorded and the period of time in which the use of the device is authorized, including a statement as to whether or not the use shall automatically terminate when the described conversations have been first obtained.

(b) An order authorizing the use of an eavesdropping device shall, upon the request of the applicant, direct that a communication common carrier shall furnish the applicant all the information, facilities, and technical assistance necessary to effect the order with a minimum of interference with the service of that carrier. Such carriers shall be compensated by the applicant at reasonable rates.

(c) No order entered under this section may authorize or approve the use of any eavesdropping device for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than 10 days. An initial or a subsequent extension, in no case for more than 10 days each, of an order may be granted but only upon application made in accordance with Section 108A-3 and where the court makes the findings required in Section 108A-4.

(Ch. 38, par. 108A-6).

Sec. 108A-6. Emergency Exception to Procedures.

(a) Notwithstanding any other provisions of this Article, any investigative or law enforcement officer, upon approval of a State's Attorney, or without it if a reasonable effort has been made to contact the appropriate State's Attorney, may use an eavesdropping device in an emergency situation as defined in this Section. Such use must be in accordance with the provisions of this Section and may be allowed only where the officer reasonably believes that an order permitting the use of the device would issue were there a prior hearing.

An emergency situation exists when, without previous notice to the law enforcement officer sufficient to obtain prior judicial approval, the conversation to be overheard or recorded will occur within a short period of time and the use of the device is necessary for the protection of the law enforcement officer.

(b) In all such cases, an application for an order approving the previous or continuing use of an eavesdropping device must be made within 48 hours of the commencement of such use. In the absence of such an order, or upon its denial, any continuing use shall immediately terminate.

In order to approve such emergency use, the judge must make a determination (1) that he would have granted an order had the information been before the court prior to the use of the device and (2) that there was an emergency situation as defined in this Section.

(c) In the event that an application for approval under this Section is denied or in any case where the use of the device is terminated without an order of approval having been issued, the contents of the conversations overheard or recorded shall be treated as having been obtained in violation of this Article.

(Ch. 38, par. 108A-7)

Sec. 108A-7. Retention and Review of Recordings.

(a) The contents of any conversation overheard by any eavesdropping device shall, if possible, be recorded on tape or a comparable device. The recording of the contents of a conversation under this Article shall be done in such a way as will protect the recording from editing or other alterations.

(b) Immediately after the expiration of the period of the order or extension or, where the recording was made in an emergency situation as defined in Section 108A-6, at the time of the request for approval subsequent to the emergency, all such recordings shall be made available to the judge issuing the order or hearing the application for approval of an emergency application.

The judge shall listen to the tapes, determine if the conversations thereon are within his order or were appropriately made in emergency situations, and make a record of such determination to be retained with the tapes.

The recordings shall be sealed under the instructions of the judge and custody shall be where he orders. Such recordings shall not be destroyed except upon order of the judge hearing the application and in any event shall be kept for 10 years if not destroyed upon his order.

Duplicate recordings may be made for any use or disclosure authorized by this Article. The presence of the seal provided for in this Section or a satisfactory explanation for the absence thereof shall be a pre-requisite for the use or disclosure of the contents of the recordings or any evidence derived therefrom.

(c) Applications made and orders granted under this Article shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge requests. Such applications and orders shall be disclosed only upon a showing of good cause before a judge. Such documents shall not be destroyed except on the order of the issuing or denying judge or after the expiration of 10 years time if not destroyed upon his order.

(Ch. 38, par. 108A-8).

Sec. 108A-8. Notice to Parties Overheard

(a) Within a reasonable time, but not later than 90 days after either the filing of an application for an order of authorization or approval which is denied or not later than 90 days after the termination of the period of an order or extension thereof, the issuing or denying judge shall cause to be served on the persons named in the order or application and such other persons in the recorded conversation as the judge may determine that justice requires be notified, a notice of the transaction involving any requested or completed use of an eavesdropping device which shall include:

- (1) notice of the entry of an order, of subsequent approval in an emergency situation, or the denial of an application;
- (2) the date of the entry, approval, or denial;
- (3) the period of the authorized use of any eavesdropping device; and
- (4) notice of whether during the period of eavesdropping devices were or were not used to overhear and record various conversations and whether or not such conversations are recorded.

On an ex parte showing of good cause, the notice required by this subsection may be postponed.

(b) Upon the filing of a motion, the judge may in his discretion make available to such person or his attorney for inspection such portions of the recorded conversations or the applications and orders as the judge determines it would be in the interest of justice to make available.

(c) The contents of any recorded conversations or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other judicial or administrative proceeding unless each party not less than 10 days before such a proceeding has been furnished with a copy of the court order and accompanying application under which the recording was authorized or approved and has had an opportunity to examine the portion of the tapes to be introduced or relied upon. Such 10 day period may be waived by the judge if he finds that it was not possible to furnish the party with such information within the stated period and that the party will not be materially prejudiced by the delay in receiving such information.

(Ch. 38, par. 108A-9).

Sec. 108A-9. Motion to Suppress Contents of Recording, etc.

(a) Any aggrieved person in any judicial or administrative proceeding may move to suppress the contents of any recorded conversation or evidence derived therefrom on the grounds that:

- (1) the conversation was unlawfully overheard and recorded;
- (2) the order of authorization or approval under which the device was used or a recording made was improperly granted; or

(3) the recording or interception was not made in conformity with the order of authorization.

(b) Such a motion shall be made before the proceeding unless there was no previous opportunity for such motion. If the motion is granted, the contents shall be treated as having been obtained in violation of this Article. Upon the filing of such a motion, the judge may in his discretion make available to the moving party or his attorney such portions of the recorded conversation or evidence derived therefrom as the judge determines to be in the interests of justice.

(Ch. 38, par. 108A-10).

Sec. 108A-10. Appeal by State. In addition to any other right to appeal, the State shall have the right to appeal from a denial of an application for an order of authorization or approval and the right to appeal the granting of a motion to suppress.

Where the State appeals, such appeal shall be taken within 30 days after the date the order was denied or motion granted and shall be diligently prosecuted.

(Ch. 38, par. 108A-11)

Sec. 108A-11. Reports Concerning Use of Eavesdropping Devices.

(a) Within 30 days after the expiration of an order and each extension thereof authorizing the use of an eavesdropping device, or within 30 days after the denial of an application or disapproval of an application subsequent to any alleged emergency situation, the issuing or denying judge shall report to the Administrative Office of the Illinois Courts the following:

- (1) the fact that such an order, extension, or subsequent approval of an emergency was applied for;
- (2) the kind of order or extension applied for;
- (3) a statement as to whether the order or extension was granted as applied for, was modified, or was denied;
- (4) the period authorized by the order or extensions in which an eavesdropping device could be used;
- (5) the felony specified in the order extension or denied application;
- (6) the identity of the applying investigative or law enforcement officer and agency making the application and the State's Attorney authorizing the application; and
- (7) the nature of the facilities from which or the place where the eavesdropping device was to be used.

(b) In January of each year the State's Attorney of each county in which eavesdropping devices were used pursuant to the provisions of this Article shall report to the Administrative Office of the Illinois Courts the following:

- (1) the information required by subsections (a) (1) through (a) (7) of this Section with respect to each application for an order or extension made during the preceding calendar year;
- (2) a general description of the uses of eavesdropping devices actually made under such order to overhear or record conversations, including: (a) the approximate nature and frequency of incriminating conversations overheard, (b) the approximate nature and frequency of other conversations overheard, (c) the approximate number of persons whose conversations were overheard, and (d) the approximate nature, amount, and cost of the manpower and other resources used pursuant to the authorization to use an eavesdropping device;
- (3) the number of arrests resulting from authorized uses of eavesdropping devices and the offenses for which arrests were made;
- (4) the number of trials resulting from such uses of eavesdropping devices.
- (5) the number of motions to suppress made with respect to such uses, and the number granted or denied; and
- (6) the number of convictions resulting from such uses and the offenses for which the convictions were obtained and a general assessment of the importance of the convictions.

(c) In April of each year, the Director of the Administrative Office of Illinois Courts shall transmit to the General Assembly a

report including information on the number of applications for orders authorizing the use of eavesdropping devices, the number of orders and extensions granted or denied during the preceding calendar year, the convictions arising out of such uses, and a summary of the information required by subsections (a) and (b) of this Section.

MR. GILLIS: It, in effect, takes the controls that are in Section 2518 of the Federal law and requires those for consensual overhearings under our law and would make it necessary for us to obtain the prior application of a judge before we could use consensual eavesdropping or overhearing.

This, as Mr. Busch said earlier, is the sort of limitation that would make impractical the use of the recording when you look at the practical problems that a law enforcement officer faces in gathering this type of evidence.

The person who is operating in narcotics simply doesn't stay put to allow you to specify times and places and exact facts of what is going to go on before the occurrence.

As the Commission knows, these criminal endeavors frequently are consummated on short notice under conditions not always known by the law enforcement officer until the very end. You are not dealing here with dumb people. Organized criminals are people who make their livelihood from crime. They are extremely wary and they know how to defeat the means that law enforcement has available to it.

So I think this sort of requirement of the application as set out in the interception area hinders us when we are dealing with the consensual overhearing.

As with any law enforcement tool, the areas of wiretapping or the areas of consensual recording can be abused. In Illinois, we use many controls, hopefully basically our prosecutorial discretion; ultimately, that stems any abuse of the powers that we have.

I feel very strongly that the tools that are most important to law enforcement are the ones that can be abused and, as such, if they are, can and perhaps will be taken away from law enforcement officials. We have to constantly keep that in mind in using our power, of course.

I very briefly would comment—and I suppose you will ask more questions about it—in our day-to-day activities, the crimes that we have thwarted, the prosecutions that we have made, we have seen the need for non-consensual wiretapping. We deal with this specifically and not as much philosophically as in a practical sense. We would say if we could have a warrant on that particular phone at certain hours of the evening, we could gain hard evidence of

armed robberies to happen, and other crimes of that nature. And I feel that non-consensual eavesdropping could be an invaluable aid to use in Cook County. I think it would be invaluable to anybody who has engaged in the fight against crime.

Thank you.

MR. REMINGTON: Thank you. I think the staff has some preliminary questions.

MR. LIPMAN: I would like to start by having each of you gentlemen set forth for the record your prior legal experience, particularly with regard to law enforcement.

Mr. Gillis.

MR. GILLIS: I have been a prosecutor for about 7 years and a defense lawyer for 8 years. I have been in practice for a total of 15.

I was a prosecutor in the early part of my career and came back with the present State's Attorney, Bernard Cary, in 1973. I am presently head of the Special Prosecutions Bureau which has many of the task force groups that work closely with our area police and one of them is the unit which concentrates on official crimes, and the second one, which Mr. Iavarone heads, deals with the area of organized crime.

MR. LIPMAN: And how long have you had this position?

MR. GILLIS: We have reorganized the office and I have had it about two years now.

MR. LIPMAN: And have you had any other prior experience with regard to investigative-type prosecution work?

MR. GILLIS: No.

MR. LIPMAN: Mr. Iavarone.

MR. IAVARONE: I came with the State's Attorney's office in February '73. I worked in the Appellate Division until the Task Forces were organized in November of '73. And I became the supervisor of one of the task forces in December of 1974.

MR. LIPMAN: December of —?

MR. IAVARONE: 1974.

MR. LIPMAN: And that is the extent of your experience as a prosecutor, also?

MR. IAVARONE: Yes.

MR. LIPMAN: There are several things you have touched on in your statement, Mr. Gillis, that I would like to go back to, but so the record is clear on several points I think we ought to just briefly give a description of the jurisdiction you are working in, that is, Chicago, with regard to what investigative tools are legally available to you as a prosecutor in Cook County.

You have heard Mr. Busch testify previously as to the use of grand juries in Los Angeles. Can you use grand juries in Cook County as investigative grand juries, and do you do so.

MR. GILLIS: Yes, we can and we do.

MR. LIPMAN: Am I correct in saying that Illinois State law requires that all felony trials or all felonies must be processed by a grand jury and must have a grand jury indictment before they can be tried?

MR. GILLIS: That's the present law, yes. We have sponsored a so-called by-pass bill which would allow us, after a finding of probable cause, to move automatically by the grand jury in those cases, which would be the vast majority of crimes that we would be dealing with—if the bill passed the Legislature we would be able to move on felonies without going through the grand jury.

MR. LIPMAN: But now all felonies must go through the grand jury?

MR. GILLIS: Yes.

MR. LIPMAN: Approximately how many felonies a year are processed by the Cook County Grand Jury?

MR. GILLIS: Last year we had 7,000. So, as your question senses, the Grand Jury procedure is hectic. I would suppose true bills are voted on the average every three or four minutes through the course of a day, and it is a very summary procedure, which is why we asked that a by-pass mechanism be set up.

MR. LIPMAN: Now, by statute, Mr. Gillis, how many grand juries may there be sitting in Cook County at any one time?

MR. GILLIS: We are allowed six.

MR. LIPMAN: And in practice how many grand juries sit in Cook County at any one time?

MR. GILLIS: Well, I would suppose it would be around four. We keep a little leeway, if some crisis comes up. But I would suppose on the average it is about four.

MR. LIPMAN: That is four grand juries impaneled at once?

MR. GILLIS: Yes, at any one time. They would not be sitting on any given day.

What we do after their normal term of 30 days of hearing of what might be described as finite types of crimes or street crimes that are isolated in time and place is to extend the grand jury to deal with a limited number of more complex, lengthy investigations—perhaps two or three concerns of that nature. And they would come back at the will of the prosecutor and at the convenience of the grand jury, perhaps one day a week or two days every other week, something of that nature.

MR. LIPMAN: But they would not be sitting on a daily basis?

MR. GILLIS: They would not.

MR. LIPMAN: That is what is commonly referred to as a hold-over grand jury?

MR. GILLIS: Yes.

MR. LIPMAN: Is it correct in saying that if a member of your particular staff, Special Operations staff, was in the middle of conducting an investigation into organized crime or into corruption, whatever, that access to a grand jury is tremendously limited unless that grand jury is going to be a hold-over grand jury?

MR. GILLIS: Yes.

MR. LIPMAN: In other words, if in the month of June—am I correct in saying that only one grand jury will be impaneled for the month of June?

MR. GILLIS: Yes.

MR. LIPMAN: And if you have an investigation that begins on June 10, in all likelihood you will not be able to get substantial jury time until the last day in June when the grand jury is held over, and then the subsequent months after that?

MR. GILLIS: Yes. We ask that all major crimes be committed towards the end of the month for our convenience.

MR. LIPMAN: Has any attempt been made by your staff to have the presiding justice or the administrative justice impanel a grand jury or several grand juries to hear corruption and organized crime cases?

MR. GILLIS: Yes. Our statute permits us, we thought, the power to petition for a special grand jury to deal with concerns of that type. But our chief judge ruled against us and the Illinois Supreme Court affirmed his decision.

So we are dealing basically within the discretion of the chief judge.

MR. LIPMAN: Who appoints the chief justice—the chief judge of the court?

MR. GILLIS: Well, we are actually dealing with the chief judge of the Criminal Division and I think he is selected by the chief judge within the county who is elected by the rest of the circuit judges.

MR. LIPMAN: Just so it is clear for the record, the present State's Attorney in Cook County is of what political party?

MR. GILLIS: He is a Republican.

MR. LIPMAN: And I guess we can take judicial notice of the party of the Mayor of Chicago.

Mr. Busch testified previously with regard to problems of immunity grants in investigative grand juries.

Does Chicago have an immunity statute that you can utilize in investigative grand juries?

MR. GILLIS: Yes, we do. But I think Mr. Busch was correct in his appraisal that that is not the answer to many types of crimes. Our experience has been that a grant of immunity—with that, an organized crime type figure is going to avoid, generally, the area that you are interested in, or obstruct you when you get to that area if you have the ability to place a perjury case against him.

So it is very, very difficult to gain the type of evidence about standing and operating criminal conspiracies, in my mind, from the immunity statute.

MR. LIPMAN: Is your immunity transactional or testimonial or both?

MR. GILLIS: It is transactional.

MR. LIPMAN: Does Illinois have a corroboration statute?

MR. GILLIS: Well, it is not a statute but it is by judicial opinion. I consider that we would have to have detailed corroboration of an accomplice or someone to grant immunity.

MR. LIPMAN: Do you have a contempt proceeding in Illinois available to you that is analogous to the New York State contempt, whereas, if a witness refuses to testify in a grand jury he may be indicted for the felony of contempt rather than the usual contempt proceeding of jailing the witness until the termination of the grand jury?

MR. GILLIS: Ours is the traditional proceeding which can carry with it the penalty up to the life of the grand jury, which would be 18 months.

But in practice that is very difficult, I believe, to use as a deterrent to obstruction before the grand jury.

MR. LIPMAN: I'm sorry. I didn't hear that first part. Would you repeat it?

MR. GILLIS: I don't believe that the possibility of contempt for the life of the grand jury is a deterrent to obstruction of justice by a witness before the grand jury.

MR. LIPMAN: So, for example, if a witness were to refuse to answer, he would be subject only to 30 days imprisonment, assuming that the grand jury would not be held over?

MR. GILLIS: That is right.

MR. LIPMAN: Let me skip now to a question regarding personnel in your office.

When the staff interviewed some of the people in your office, it was indicated that the experience level of the attorneys in your Division, Organized Crime and Corruption, is substantially lower than that of most other large city units of comparable jurisdiction.

MR. GILLIS: Yes.

MR. LIPMAN: One, would you say that is a fair assessment and, two, could you give us an indication of perhaps why that is?

MR. GILLIS: Well, it is a fair assessment. I do not know exactly why it is. Perhaps it is some sort of throw-back in Cook County that it is not wise to prosecute organized crime. I hope that is not true.

Whether it is because I head a new bureau that doesn't have the tradition of some other types of offices in other areas, perhaps might be a part of it.

But what we lack in years of experience, I think we make up in the fervor with which we go at the activities against organized crime.

MR. LIPMAN: Mr. Gillis, is it correct—just so the record is perfectly clear—that the average experience level of your attorneys—and I mean within your bureau—is just a little over a year as a prosecutor?

MR. GILLIS: Yes. We have tried various techniques, although we don't have attorneys of the amount of years of experience that I would like—four, five, or six years' experience—but in trying people of lesser experience than that, I found more success with attorneys out of law school that have a fresh perspective to the problem and are eager to get going.

MR. LIPMAN: Is it correct, Mr. Gillis, to say that you have attempted to embody the Strike Force concept that Professor Blakey was referring to previously with Mr. Busch, in your unit?

MR. GILLIS: Yes.

MR. LIPMAN: That is, the close cooperation between investigators and prosecutors at an early stage of a major investigation?

MR. GILLIS: We do that in the areas of street crime, felonies such as murder, armed robbery, burglary, with one unit. And then units in my bureau work on more involved, complex financial crimes and organized crimes. Yes.

MR. LIPMAN: For the most part, where do you draw your investigators from?

MR. GILLIS: Well, we are cooperating with the police in the area, largely the units of the Chicago Police Department, some suburban police, the Illinois Bureau of Investigation.

Within our office we have about 50 civilian investigators who are not trained policemen. They are college graduates. That is the educational requirement that we have on those positions.

They lack experience. We had police assigned to us from the Chicago Police Department. They were withdrawn in 1973 and we have been building upon the base of these civilian investigators since then.

MR. LIPMAN: When you say you "had police," is it correct that you had approximately 70 officers from the Chicago Police Department attached to the State's Attorney's Office for use in precisely this type of investigation?

MR. GILLIS: Yes.

MR. LIPMAN: Who were experienced police officers?

MR. GILLIS: Yes, and they had been since I can remember—at least 20 years.

MR. LIPMAN: And you say they were withdrawn in 1973. Was that at about the same time or coincidental with the election of the Republican State's Attorney?

MR. GILLIS: Yes.

MR. LIPMAN: Let me turn now to the problem of consensual wiretapping.

As referred to before, the Illinois statute requires that before a consensual monitoring can be implemented, the permission or at least the request must be obtained from a State's Attorney; is that correct?

MR. GILLIS: Yes.

MR. LIPMAN: And again staff interviews indicated—and please correct me if I am wrong—that at least in the Cook County area that statute has been interpreted to mean the State's Attorney, himself, rather than an assistant State's Attorney?

MR. GILLIS: Yes.

MR. LIPMAN: Whereas, in the downstate area it has been interpreted to mean the request comes from the Assistant State's Attorney?

MR. GILLIS: Yes. I think that is important in our attitude about this evidence.

It seems to me clear that if you require the permission of one person, the chief prosecuting attorney, you are accomplishing substantial controls by that means. You are putting accountability for this type of evidence squarely on a prominent public official who has been elected, presumably would stand for election again. And I think that brings you the type of control that is desirable in this area.

We could have, I suppose, interpreted the statute as meaning any of our 330 assistant State's Attorneys, but obviously that would lead to, I think, chaos if everybody felt they had the power to give approval to the use of this sort of equipment.

I am proud of our techniques that we have set up to control this sort of evidence. The law enforcement officials in the area, if they desire to use this sort of evidence, come to me. The law book that controls applications for these is in the bottom right-hand drawer of my desk. The attorney will put the lengths of time that are required to use this equipment, and we insist on finite amounts of time, periods of days. We seldom go over three days in time.

And we do these things not only in anticipation of arguments that defense attorneys might bring up, but also because I am convinced that strict care in using this equipment is important if we are to be allowed to continue to use technology to help fight crime.

MR. LIPMAN: As long as you have begun to enumerate the procedures, I would like to set them forth completely, just so it is clear.

Are you saying that any investigative officer in Cook County who wishes to utilize a consensual monitoring device in Cook County must come at least to your bureau and get permission through

your bureau, whether you are available or Mr. Iavarone or his counterpart, and you will then check with Mr. Carey, the State's Attorney?

MR. GILLIS: Yes.

MR. LIPMAN: And I believe that, as indicated in the documents submitted for the record, where there are two samples received from your office, that authority from Mr. Carey or that request from Mr. Carey can be either his actual signature or telephone approval?

MR. GILLIS: Yes.

MR. LIPMAN: But it always comes from Mr. Carey?

MR. GILLIS: Yes. If possible, we try to reach the State's Attorney throughout the county or the state, tell him the facts of the case, what amounts to probable cause information. This is communicated to him. We tell him the times that we are requesting, the persons involved if we know them; if we do not know them, some description of the unknown person. And we get his approval or rejection of the request.

MR. LIPMAN: You have articulated in your last response what seemed to be several standards that you are looking for and several bits of information that you seem to require to go into this documented request.

One of them, I believe, is time?

MR. GILLIS: Yes.

MR. LIPMAN: Do you have any statutory time limit on the length for which consensual monitoring will be legitimate?

MR. GILLIS: We have no present statutory requirement. The bill I mentioned, House Bill 212, sets a ten-day rule. And we have one appellate court opinion that rules that seven days is too long within the facts of that case.

So, basically we are dealing with periods of time less than seven days.

MR. LIPMAN: So, for example, if you were conducting, as I believe is presently going on in Cook County, a long-range undercover investigation which utilizes consensual and monitoring devices, there must be recurrent and continuous applications to the State's Attorney and approval of the State's Attorney?

MR. GILLIS: That is right.

MR. LIPMAN: Does that cause any problems, or has it so far?

MR. GILLIS: It is time-consuming and it is laborious, but it has not caused any serious problems. We update these twice a week and add new persons who come into the scenario, and describe them as best we can as we go along.

MR. LIPMAN: You just mentioned the second factor I would like to discuss, and that is naming the persons who are going to be intercepted.

Again the question is two-part.

One, is there either a statutory or a case law requirement that these persons be listed? And, if not, has your office established a requirement that you name the persons who are going to be intercepted?

MR. GILLIS: There is no statutory requirement at the present time. There are some suggestions in a couple of legal opinions that litigated the issue of whether the tapes should be suppressed or allowed into evidence. That description should be made. So we try to anticipate problems, of course, and try to describe either by name or other means.

I should comment, I think, that I think it is vital that that information be kept within the prosecutor's house, because there is obviously a danger, if application of that type is being made in a court—perhaps no different from a search warrant, but our present bill requires, or at least allows in some instances, a hearing on whether the judge should allow permission for overhearing.

When you are dealing with problems of time and problems of filing documents, you of course jeopardize the success of the operation and jeopardize the identity of your agents.

MR. LIPMAN: Would that be an ex parte hearing?

MR. GILLIS: It would. But I think any lawyer knows that any hearing that goes on—the word gets out pretty quickly what exactly is happening.

MR. LIPMAN: Thirdly, let me ask you this. Again, the same two-part question: Is there any legal requirement or any requirement imposed by your office to name the persons specifically who are going to do the monitoring in that request?

MR. GILLIS: That is another theme that was in an appellate court opinion, and we follow that directive and memorialize the people who are working with the equipment or overhearing it or are in any way connected with it.

MR. LIPMAN: To this date has there been suppression of any evidence seized through use of a consensual monitoring because either the time period was too long or the persons being intercepted were not named in the formal request or the persons doing the monitoring were not named in the formal request?

MR. GILLIS: Yes. We have lost only one case at the appellate court level, though.

MR. LIPMAN: That was the time factor?

MR. GILLIS: Yes. But decisions that we have lost at the trial court we have won at the appellate level.

MR. LIPMAN: Have you lost any trial court decisions based on naming persons either to be intercepted or to do the intercepting?

MR. GILLIS: I am not sure we have had that exact problem, but we have had others.

MR. LIPMAN: What are the others?

MR. GILLIS: Time—general constitutionality of the statute. But I don't think we have been faced with the naming of the persons involved.

MR. LIPMAN: Are you saying that you have had evidence suppressed on a constitutional argument?

MR. GILLIS: Yes, we have had evidence suppressed, the judge ruling the entire statute was unconstitutional. The Supreme Court, however, held the statute requires more protection for the individual than would exist without statute, so the trial judge was reversed and the statute was found to be constitutional.

MR. LIPMAN: When a police officer walks into your office and sits down and says, "Mr. Gillis, I have a problem here in an investigation and I would like permission to utilize a consensual monitoring device," have you ever refused permission, or has permission ever been refused by Mr. Carey?

MR. GILLIS: Yes, we have refused requests.

MR. LIPMAN: On what grounds have you made your refusals?

MR. GILLIS: Let's see if I can think of them all.

I suppose the practical one that comes up most is whether the use of the device is going to be effective, whether it is a possibility or a probability that hard evidence is going to be gained by the use of it, or whether it is a policeman's hope of avoiding some legwork that he should do.

I feel that in all areas, when you are dealing with a new device or a new statute, there may be a knee-jerk reaction, "Boy, this is what we need in order to solve the case."

And I think we need to be a little hard-headed about use of any new technique and ask whether it is really necessary.

I don't like to allow somebody to go off on a path if we are not going to get some fruitful evidence from it.

Secondly, use of a recording device almost necessarily means that the person who wears the tape recorder is going to become a state's witness. And extreme care has to be used, in my mind, to see who we are marrying, as it were. If it is someone who has some culpability, I want to know about that and I want a divorce very early in the proceedings. I don't want to get linked up with somebody we are not convinced in the long run that we would, say, grant immunity to, or in effect pass for his activities.

Those are two.

The third one really is—I suppose that is largely the first one.

Excuse me.

[Discussion off the record.]

MR. GILLIS: There are some problems often-times. Mr. Iavarone mentioned one where we had two agencies involved, the Narcotics Agency and some suspicion that a narcotics agent was involved in some impropriety and we were faced with the either comic or tragic possibility that two people, one authorized by a federal agency and one by us, would be taping each other's conversations.

I think that is comic and tragic because it shows sometimes a non-smart or non-intelligent use of this equipment and not thinking of where we are going when we authorize it.

Incidentally, that instance never did happen. That was one instance where we did not allow the agency to have it.

MR. LIPMAN: Mr. Gillis, do you in fact impose some sort of probable cause standard before you approve one of these consensual monitorings?

MR. GILLIS: Yes. And I think that is extremely important, because we have had some instances within our city years ago when anti-war feeling was high and people were protesting, and where perhaps autonomous units of the police department saw a threat in excess of what it turned out to be now, but what at the time was viewed to be very serious, where police agencies were investigating community organizations and other organizations which could not under any conceivable notion be committing the types of crimes that should be the target of this sort of evidence.

When you have that, when you have police that don't define the danger, don't define the area that they are dealing with, that they are infiltrating, it brings about a misunderstanding that affects all of us, that could take away from us the powers that we need to fight crime.

MR. LIPMAN: So what I take it you are saying is that you feel it is important for a prosecutor, at least, to sit as kind of a watchdog over the police in their use of electronic surveillance?

MR. GILLIS: Yes.

MR. LIPMAN: You think that is an important function for a prosecutor to play?

MR. GILLIS: Very definitely.

MR. LIPMAN: In addition to the other problems that you have talked about, that a person who is wearing a consensual device would in all likelihood become your own witness and you would like to have some control over the case at an early date?

MR. GILLIS: Yes. Let me perhaps give you one short example of that that shows you how easily this thing can swing.

We had a matter under investigation where a suburban policeman was accused of brutally assaulting a citizen, and the citizen had the bumps and bruises and more to back up his allegation that he was brutalized.

Shortly thereafter, the police chief of that suburb came to us and said "We feel that there will be some obstruction of justice or some bribery on the part of the citizen or his family in connection with that police officer." The citizen, in addition to the physical damage, was charged with resisting arrest or something of that nature.

And if we were to have approved that, the use of the device on that police officer to see whether the citizen or his family would come forward, we would in effect be saying, it seems to me, that there was no case against the policeman, that there was no valid case that could be made against the policeman.

And I think that too often, perhaps, a prosecutor would jump in and say "Well, sure, you can wear the recorder and see what evidence comes forward."

But I think that would be kind of a critical stage in evaluating whether a prosecution is to go ahead against Party A or Party B. And it was simply too early to tell. So we refused it in that instance.

MR. LIPMAN: I would just like to move on now. I know members of the Commission probably have questions they would like to ask about consensual monitoring, but there are two other areas I would like to talk about.

One, briefly, is the investigation into illegal wiretapping. And let me ask you two questions.

One, has your office been involved in investigating illegal wiretapping by private citizens?

And, two, has your office been involved in investigating illegal wiretapping by police?

MR. GILLIS: I don't think we have had any cases involving private citizens. Of course that danger exists and there is strong suspicion, if not evidence, that there are private investigators and others who have the wherewithal to use this technology for themselves for illegal means.

We have a grand jury investigation, that I alluded to earlier, involving the Chicago Police Department and their infiltration of organizations and use of illegal wiretapping equipment. It is relatively easy, I was surprised to find out, to find out what wire on the telephone pole goes to which home. It is simply a matter of finding the little number, getting a telephone company code book that says what number matches to what 7-digit number in a person's house, and connecting a wire and listen to the line.

I can share this evidence with you, that a Chicago police officer in his function of surveilling groups did such illegal eavesdropping.

I am not saying that is widespread. In fact, our evidence has indicated that it is a rather small, quote, intelligence unit of one bureau within the

Chicago Police Department. But it is a subject of concern and a subject of our grand jury investigation.

MR. LIPMAN: What tools are available to you to investigate the illegal wiretapping that has taken place, I am assuming, four, five, or six years ago?

MR. GILLIS: Well, that is very difficult, anything that has occurred a long time ago, of course. We have had large success using the grand jury and our perjury statute, so that in many instances we are able to prove, through outside means, that something did occur and a witness will say that it did not, and that gives you a present, 1975, crime of perjury before the grand jury.

MR. LIPMAN: So what you are talking about is almost what we were talking about with Mr. Busch, immunizing a witness, bringing him before the grand jury and putting him in that contempt-immunity vise and forcing him to choose between testifying or subjecting himself to contempt.

MR. GILLIS: If you are able to get material facts that you can contradict a witness on, you can ideally make a perjury case.

That does not apply to an unconsummated crime. It works well in an ongoing criminal conspiracy such as narcotics sales or things of that nature.

But one instance you will undoubtedly ask Mr. Iavarone about is that we had a crime about to occur. We didn't know where. We knew some basic guidelines about it through an agent informant. But of course we could not bring that witness before the grand jury because we would then uncover that we were onto the activity and they would seize them.

MR. LIPMAN: As long as you have referred to Mr. Iavarone and the case, I will turn to that.

I believe you said in your opening statement, Mr. Gillis and Mr. Iavarone, both of you, that you felt there were certain types of situations where the need for non-consensual electronic surveillance has manifested itself, and you believe that it would be greatly beneficial to prosecutors and investigators in Illinois if this tool were available to you, again assuming it were under the Federal guidelines of Title III. Is that correct?

MR. GILLIS: Yes, that is correct.

MR. LIPMAN: When the staff was in your office, I believe Mr. Iavarone said there was one particular case which he felt typified the kind of situation where non-consensual electronic surveillance would be useful, and I would like to review the fact pattern of that particular case.

The staff report on Chicago has been introduced elsewhere into the record, and I believe there is about a 6- or 7-page summary of that case, which is entitled The Purolater Case.

Mr. Iavarone, could you briefly give us some background as to what this case was about and how it began?

MR. IAVARONE: Yes. Well, the report says in the spring of 1974 our office, the Illinois Bureau of Investigation and the Illinois Investigating Commission, began an operation to look into the fencing of stolen goods through discount stores in Chicago, and the whole Cook County area.

In doing so we had an informant and some undercover personnel that, themselves, posed as fences. And since ourselves and the Commission did not have a large amount of money to go into a large fencing operation, we gained the cooperation of private firms who would supply us with money and goods.

MR. LIPMAN: Let's explain that. Because, when you first indicated that to me I was somewhat confused and I want to make sure the Commission is clear on that.

You decided to undertake an undercover operation; is that correct?

MR. IAVARONE: That is correct.

MR. LIPMAN: Whereby you were going to use an informant and several undercover agents to infiltrate and set up a fencing operation in Cook County; is that correct?

MR. IAVARONE: That is correct.

MR. LIPMAN: And I think by now everybody is clear a fencing operation is an operation which deals with the buying and selling of stolen goods.

MR. IAVARONE: That is correct.

MR. LIPMAN: And I am assuming we are talking about a major-type operation, not of the Mom and Pop variety, stealing a junkie's proceeds from a burglary, but rather about an operation that is handling significant shipments of stolen goods, either from truck hijackings, larcenies from the docks, freight yards and railroads, things like that.

Is that correct?

MR. IAVARONE: Yes.

MR. LIPMAN: Now, where did you get the money to finance the operation which would enable you to purchase stolen goods?

MR. IAVARONE: Well, first we would get goods that our undercover people would have and would say they were stolen goods from manufacturing concerns, who would sell them to us at cost. And then we would sell them at cost to these discount houses so we wouldn't lose any money.

That was the way you got in the door to most of these operations.

MR. LIPMAN: So, in other words, you would go to a company, let's say X Company, who might be selling razor blades, and purchase from this company at cost 10,000 or 5,000 dollars worth of razor

blades. And then your undercover agent would pose as a thief and go to a fence and say "I've got \$10,000 worth of stolen razor blades. Would you like to buy them?" and the people would then buy them from your agent at \$10,000 and that is how you were financing the operation at that stage?

MR. IAVARONE: That is correct. Then, these individuals, of course, would have stolen merchandise of their own. It usually worked in one of two categories: First of all, employee thefts, where you have a company and the fences are dealing in a large amount of their goods which are being stolen off their docks. The companies, in order to find out, first of all, who was stealing, how it was being done, and to better improve their own security, would give us money to buy back those goods.

The other group would be insurance companies who had suffered a loss in transit or somewhere else, and that would then give us the money to also buy back their goods. And that is how we were able to finance the operation.

MR. LIPMAN: So, for example, if the insurance company's policy called for them to pay out \$10,000 in goods that were stolen, they would give you the \$10,000, you would buy the goods and return the goods to the insurance company—

MR. IAVARONE: That is correct.

MR. LIPMAN: —who would then reimburse—

MR. IAVARONE: Or give the goods back to the company.

MR. LIPMAN: About how long did it take you to establish your undercover situation in the business itself?

MR. IAVARONE: I would say about six weeks. We started dealing with a number of discount stores. The informant, who had been known in the business as previously owning this kind of store, then went to work for one of the larger discount stores in accounting. That individual was dealing in a number of stolen goods, different types of merchandise. And through the informant we were able to introduce him to the undercover people who were posing as fences and there were transactions back and forth.

All of these transactions were recorded with the consent of the undercover individuals.

MR. LIPMAN: So your undercover people were putting body microphones on and recording the sales?

MR. IAVARONE: Either that or telephone conversations. They would engage in telephone conversations with the owners of the discount stores and those would be recorded.

Later, about a month and a half after that, the informant was introduced to an individual that wanted to open a discount store. That individual

wanted the informant to work for him. And that member was a member of organized crime. And through the informant we were able to get some information as to what was going on, through the conversations he had with the person he was working for.

Many of the things he wouldn't tell him. He would tell him only bits of information. The informant sometimes would catch part of a telephone conversation—of course, the half where the person he was working for was talking—or was told that certain meetings were going to occur, to drive this individual to a meeting, what the general subject of the meeting was and who was attending—but not what went on in the meeting.

MR. LIPMAN: Again, let me sum up here so it is clear.

After your undercover business was established, at some point your actual original informant was introduced to or began working for a fence who was operating a discount store or was about to open a discount store, who was ostensibly a member of organized crime; is that correct?

MR. IAVARONE: That is correct.

MR. LIPMAN: Now, at that point had you decided to terminate the investigation, you could have made numerous arrests for possession and sale and interstate transportation of stolen property; is that correct?

MR. IAVARONE: That is correct. We could have made some arrests for receiving stolen property and turned over to Federal authorities information on interstate transportation.

MR. LIPMAN: And without any possibility of wiretapping, at this point anyway, with regard to this gentleman you say was involved in organized crime, did you make any direct sales to him or purchases of stolen property from him?

MR. IAVARONE: Yes, we did.

MR. LIPMAN: So at that point he could have been arrested for receiving stolen property?

MR. IAVARONE: That is correct.

MR. LIPMAN: Now, the informant actually went to work in a discount store, itself; is that correct?

MR. IAVARONE: Yes, he did.

MR. LIPMAN: And there was a telephone in that store?

MR. IAVARONE: Yes, there was.

MR. LIPMAN: And did you say the informant on several occasions overheard phone conversations on that phone between his boss, the member of organized crime, and unknown third parties?

MR. IAVARONE: Yes, he did.

MR. LIPMAN: And what was the nature of those conversations?

MR. IAVARONE: A few of them were about a planned burglary or robbery. Others were financial dealings, illegal financial dealings.

MR. LIPMAN: Illegal financial dealings?

MR. IAVARONE: Yes.

MR. LIPMAN: Of what type?

MR. IAVARONE: Stocks—stolen stocks and securities.

MR. LIPMAN: The member of organized crime was attempting to procure stolen stocks, or was he trying to sell stolen stocks?

MR. IAVARONE: He was trying to sell them.

MR. LIPMAN: And do you know where he was trying to sell them?

MR. IAVARONE: No.

MR. LIPMAN: Did you know to whom he was trying to sell them?

MR. IAVARONE: We did not.

MR. LIPMAN: But it was clear from the informant's information to you that at that point there was an illegal deal in the making for the sale of stolen securities?

MR. IAVARONE: Yes.

MR. LIPMAN: And that information came to you through information the informant had overheard on the telephone?

MR. IAVARONE: Yes.

MR. LIPMAN: Was there any other information that you had at that point?

MR. IAVARONE: We knew that people the informant was working with had been getting stolen goods, but we didn't know who they were getting them from. There would be telephone calls made and then a few days later they would get the goods. But we didn't know who was supplying the goods to the fences we were dealing with—that individual and other individuals.

When we were able to determine, in the instances that we were, we were able to find the people who were stealing from the docks or the interstate shipments.

But then they would just make a phone call—

MR. LIPMAN: Who is "they"?

MR. IAVARONE: The people who ran the discount store, the member of organized crime and others. And the goods would be at a certain location but the other individuals would not be. You wouldn't know who brought the merchandise.

MR. LIPMAN: And was your informant present and did your informant overhear at least one end of the conversations in which these goods were ordered?

MR. IAVARONE: On quite a number of occasions he did.

MR. LIPMAN: So that your informant, in fact, had overheard numerous conversations that were

clearly illegal in nature about specified crimes, that is, fencing, disposition of stocks, and believed there was also something involving some kind of financial dealing in a gold scheme, the selling of gold or something along those lines?

MR. IAVARONE: Yes.

MR. LIPMAN: All of which conversations were overheard in part by the informant and the informant could have testified or at least have submitted an affidavit to that extent had you been able to obtain a wire; is that correct?

MR. IAVARONE: Yes, he would have been and two of the undercover agents at different times would, also.

MR. LIPMAN: Was there also an indication that these same persons who were involved in the gold scheme, the stock scheme, and the fencing, were also involved in selling or trying to obtain untaxed cigarettes from North Carolina?

MR. IAVARONE: Yes.

MR. LIPMAN: Was that also clear on the telephone?

MR. IAVARONE: Yes, from two long distance telephone calls that were made.

MR. LIPMAN: Was it also clear that part of the securities deal was taking place in New York City and part in Los Angeles.

MR. IAVARONE: At least preparations were.

MR. LIPMAN: And again, that is also clear from the phone call where your informant indicated he had seen or recognized the area codes?

MR. IAVARONE: Yes.

MR. LIPMAN: Did there also come a time when the member of organized crime and his partner began discussing a, quote, "big score"?

MR. IAVARONE: Yes. That was later in the year, into September. Of course, it was just "a big cash score." And again, while the informant was there preparations or certain preparations were made by telephone, where he overheard part of the conversation but we didn't know who the individual was calling or what the other arrangements were.

MR. LIPMAN: Were there any other indications from your informant or from your undercover people that any other telephones were being used? For example, was there ever an instance when the member of organized crime would indicate to your informant that he was using his home telephone to further his criminal activities?

MR. IAVARONE: There would be instances where the informant, as cautiously as he could, would ask questions regarding different transactions that were going on, and this person would then say "I will know that after I call tonight." Sometimes he would be making calls on different deals the same night, from his home.

MR. LIPMAN: Did there ever come a time when your informant called his boss at home and was told that he really couldn't talk now, that he had a lot of phone calls to make about a lot of important deals and he would get back to him at a later point?

MR. IAVARONE: I think on three or four occasions that occurred.

MR. LIPMAN: Was there any time when any part of that discount store was being utilized as a meeting room by other people who have been identified as members of organized crime in Chicago?

MR. IAVARONE: The small back room was used extensively by three members of organized crime—upper echelon, and the person whose store it was.

MR. LIPMAN: And what use was that back room being put to, to the best of your knowledge?

MR. IAVARONE: From what the informant had been able to hear before they went into the back room, a lot of it was discussions as to stolen goods transactions, interstate shipments.

MR. LIPMAN: Was the informant ever permitted to sit in on any of these meetings?

MR. IAVARONE: No, he was not.

MR. LIPMAN: Is there any way in which law enforcement personnel could have discovered what was going on in that back room other than by utilizing an electronic surveillance device in the back room?

MR. IAVARONE: We had attempted on some occasions with this discount store and other discount stores, where the types of merchandise at least were discussed before the people went into the meeting. But you get a generic term.

For example, let's say "refrigerators" or something, and that is all you know they are dealing in. You don't know if they have been stolen yet. Or if they have been stolen, you don't know the company. Or if they have been taken off the docks, it may have been two or three months before the company knew. So we would try to find out if there had been a theft at this time or where the goods were taken from, but we were unable to do that.

MR. LIPMAN: And after these meetings would break up, was your informant ever given any partial information as to what had transpired in the meetings from his boss?

MR. IAVARONE: As much as the boss wanted him to know—not detailed information.

MR. LIPMAN: But enough information to indicate that criminal activities were being discussed in that back room by those members of organized crime?

MR. IAVARONE: Yes.

MR. LIPMAN: Were there any investigative techniques available to you that would have enabled you to discover any of the other parties, any of the third parties involved in any of these illegal schemes?

MR. IAVARONE: I don't think so. One of the things we attempted to do or thought about doing, I think, was to subpoena the phone records. But again you have to wait until the billing date.

On some of these situations where they are talking about goods moving within a week or two weeks, we were four weeks or five weeks off from the billing date to get the long distance records to even know who the person was talking to.

If it was a situation where goods were to be delivered to the fence, we could use surveillance. But in many cases he would order then and when they were already at a location tell us, or tell the informant or the undercover people, where the goods were. So you had no way of tracing where they came from.

MR. LIPMAN: In any event, in many instances you would at best, even if you could obtain physical surveillance, be in a position to only surveil the lower echelon people actually conducting the operation?

MR. IAVARONE: That is correct.

MR. LIPMAN: Similarly, if you could obtain the phone number and ascertain the identity of someone in Los Angeles who might have been involved in the stolen securities, the only evidence you would have was that the telephone in his house was used for communication with your man in Chicago, and nothing more?

MR. IAVARONE: That is right.

MR. LIPMAN: So therefore, would it be accurate to realistically say that even if you were able to obtain his identity and subpoena him to Cook County grand jury, with the amount of evidence you have available to you at that point, would it not have been a futile gesture?

MR. IAVARONE: I would say so.

I would like to say, too, one of the reasons in this area that it is so hard to trace stolen goods—on the occasions we were able to find out who was taking them, most of the items the people dealt with were not serialized. And when we were able to find out who they were dealing with at the companies, then you have an opportunity to surveil the people as they are taking it out of the company.

For most of the items, relatively inexpensive items in large quantities, once they got away from the company or off company trucks, it was very difficult to prove they were stolen because the companies couldn't identify them. And that was one of the major obstacles we had.

MR. LIPMAN: And of course if you had a telephone wiretap installed at that point and could utilize the defendant's own words to prove that they were stolen, that would have greatly facilitated that?

MR. IAVARONE: Yes, it would.

MR. LIPMAN: There came a point, did it not, when that "big score" became the overwhelming topic of conversation in regard to the members of organized crime; is that correct?

MR. IAVARONE: I wouldn't say "overwhelming." It became more frequent, up to a point.

MR. LIPMAN: And what exactly did you know about this "big score?"

MR. IAVARONE: There was going to be a large cash score. It was going to happen in October or November. We didn't know where; we didn't know when. We knew two of the people that were supposed to be in on it.

MR. LIPMAN: And how did you know those people?

MR. IAVARONE: From what they told the informant.

MR. LIPMAN: Was there any indication that they were utilizing the telephone to make plans for this score?

MR. IAVARONE: Yes, there was. From conversations, part of the conversations, overheard by the informant.

MR. LIPMAN: And, again, these were the same phones and the same people he had been talking about for a period of three to four months?

MR. IAVARONE: Yes.

MR. LIPMAN: And what was the result of that big score?

MR. IAVARONE: The boss had a disagreement with the informant about 13 days before and we lost a lot of communication, and were completely out of touch with these people. And it resulted in a burglary.

MR. LIPMAN: Let me go back.

Did there come a point where the member of organized crime requested that your informant obtain a truck for them to be utilized in the course of this big score?

MR. IAVARONE: Yes.

MR. LIPMAN: And did your informant actually obtain that truck?

MR. IAVARONE: Yes, he did.

MR. LIPMAN: And it was clear at that time that the truck was going to be utilized in the commission of a crime?

MR. IAVARONE: In some way it was; we didn't know in what way.

MR. LIPMAN: And did you at that point attempt to put a tracking device on the truck? Or was that considered?

MR. IAVARONE: That was considered.

MR. LIPMAN: Was it successful?

MR. IAVARONE: They eluded the surveillance before it could be accomplished.

MR. LIPMAN: So that the attempted physical surveillance on the truck failed?

MR. IAVARONE: Yes.

MR. LIPMAN: Were you attempting physical surveillance on the two members—let's call them X and Y—of organized crime we have been talking about?

MR. IAVARONE: On one of the members we were.

MR. LIPMAN: And was that physical surveillance successful? Were you able to keep him under physical surveillance?

MR. IAVARONE: Yes, it was.

MR. LIPMAN: And was there an attempt made to physically surveil?

MR. IAVARONE: No, there was not.

MR. LIPMAN: Why not?

MR. IAVARONE: It was felt that because of his capability, his intelligence, his capabilities with electronics, it would be unwise to attempt to surveil him.

MR. LIPMAN: Is it not, in fact, true that there was some fear that this gentlemen had a crystal receiver capable of picking up all police radio transmissions in the Cook County area?

MR. IAVARONE: Yes.

MR. LIPMAN: And that is one reason you didn't attempt to surveil him?

MR. IAVARONE: Yes.

MR. LIPMAN: Was it also true that he lived in a neighborhood that was essentially surveillance-proof, the type of neighborhood that any strange people coming in and sitting in that neighborhood for long periods of time would be immediately recognized?

MR. IAVARONE: It was the type of neighborhood where you couldn't get a strange car in and the type of neighborhood where you also could not get a room. Everybody would know you there.

MR. LIPMAN: So you are now sitting in the situation of an ongoing investigation in an undercover situation where you were unable to ascertain the extent of their criminal activities, the other persons involved with them in their criminal activities, and now specifically you have them talking about a particular score which you believe is some sort of theft and you are unable to ascertain exactly what it is or where it is going to happen; is that correct?

MR. IAVARONE: That is correct.

MR. LIPMAN: And what finally did happen exactly?

MR. IAVARONE: Well, they committed the theft. Of course they were subsequently apprehended.

MR. LIPMAN: I don't mean to minimize the theft by understatement. The theft that we are talking about—correct me if I am wrong—

MR. IAVARONE: —was \$4.3 million.

MR. LIPMAN: \$4.3 million of cash?

MR. IAVARONE: Yes.

MR. LIPMAN: And that was taken out of the Pulrolator—

MR. IAVARONE: Out of their vault.

MR. LIPMAN: And that was the situation in which you had prior information for at least a month about that case but were unable, through ordinary investigative techniques, to ascertain where and when and by whom that was going to occur; is that correct?

MR. IAVARONE: That is correct.

MR. LIPMAN: Now, as a result of investigation and cooperation with Federal authorities you were able to apprehend the people responsible for that particular theft; is that correct?

MR. IAVARONE: Yes.

MR. LIPMAN: Now, have you at this point been able to ascertain any of the other information we have talked about, that is the extent of any of the other schemes or the people involved in any of the other schemes?

MR. IAVARONE: No.

MR. LIPMAN: Have you recovered the full extent of that cash?

MR. IAVARONE: All but a million dollars.

MR. LIPMAN: All but a million dollars?

MR. IAVARONE: Yes.

MR. LIPMAN: Have you, to your knowledge at least, apprehended all the people who were involved in that theft?

MR. IAVARONE: I don't know if there are more people involved or not.

MR. LIPMAN: But to your knowledge you have apprehended the people who actually went into the vault?

MR. IAVARONE: Yes.

MR. LIPMAN: So it is conceivable that this operation was either financed or ordered by somebody else who you are not aware of?

MR. IAVARONE: Yes.

MR. LIPMAN: And the proceeds might have been divided among other persons who you are not aware of?

MR. IAVARONE: That is correct.

MR. LIPMAN: Is it likely that that is the case, to your knowledge or your belief?

MR. IAVARONE: To my personal belief, yes.

MR. LIPMAN: Would it be fair to say that had you had a wiretap on the several phones, or one particular phone in the store, that you would have had more complete knowledge not only of the Purolator case and those involved in that, but also the entire scope of their criminal activities?

MR. IAVARONE: I think between the two phones, yes.

MR. LIPMAN: And also let me include in that, a possible bug in that back room and even conceivably a possible bug in the truck that was ordered specifically for the crime?

MR. IAVARONE: Yes.

MR. LIPMAN: And it is conceivable, is it not, that you could have had investigators sitting in Purolator waiting for the thieves to make their attempt and not only assuring you would catch them all at the scene but recovering the extra million dollars that is now missing?

MR. IAVARONE: That is correct.

MR. LIPMAN: Now, is it true that one of the defendants in the Purolator case, in fact the gentlemen I designated before as Mr. X, has now begun cooperating with Federal authorities, or some authorities, to your knowledge?

MR. IAVARONE: Yes, to a limited extent.

MR. LIPMAN: There have been trials on the Federal level for the actual theft at Purolator; is that correct?

MR. IAVARONE: That is right.

MR. LIPMAN: And one gentleman was convicted and one gentleman was acquitted?

MR. IAVARONE: Correct.

MR. LIPMAN: One gentleman pled guilty?

MR. IAVARONE: Three pled guilty.

MR. LIPMAN: And one was convicted at trial and one acquitted at trial, that so it is clear why we are not using names, that there are multiple state indictments against all these people.

MR. IAVARONE: One had pled.

MR. LIPMAN: The rest are under indictment?

MR. IAVARONE: Yes.

MR. LIPMAN: If one person is cooperating, is there any reason why now, at this stage, you could not obtain the same information from him now that you might have been able to obtain by utilizing wiretaps or bugs previously?

MR. GILLIS: Let me answer that in general, if I could. I think this sort of witness is going to be as honest as you can make him. If you know what you are talking about and can talk to him about it, he will tell you about it. But if he thinks that you are in the dark about some part of his criminal activities, then I don't believe that a person who makes his living from crime is going to cooperate with the prosecutor or a police officer.

MR. LIPMAN: Let's just expand on that for a second.

That really is very similar to the grand jury situation where it is clear if a witness is put before the grand jury and it is made known to him that you do have the evidence to indict him for perjury if he lies, he is much more likely to tell you the truth.

MR. GILLIS: Yes.

MR. LIPMAN: Similarly here, if you had a wiretap on him and had personal knowledge of the full extent of his operation and could indicate that to him in some way, he would at that point be much more likely to open up and be honest with you?

MR. GILLIS: Yes.

MR. LIPMAN: I take it you are saying that because you had sketchy ideas of the extent of his negotiations, you were at a marked disadvantage because you did not have enough tid-bits to feed him to convince him that you really knew what he was up to and therefore he, being a sophisticated businessman, was not about to indicate to you the full extent of his participation?

MR. GILLIS: That is correct.

MR. IAVARONE: Also, I would say the opportunity is gone. The goods are gone. The people are watching out for themselves now and there are a lot of cases that, even if he were to tell everything, could not be made because the crimes are completed now, or aborted as the case may be, but the people are gone.

MR. LIPMAN: And what we have here before the Commission is a situation that appears to be analogous to the *Fraulein* case we heard, that we have a nucleus of people engaged in widespread criminal activities of different types, and whereas in *Fraulein* the wiretaps were successful in identifying other participants and the extent of the criminal activity of these people, what you have here is a situation that appears to be the same, but because you couldn't have the wiretaps you have no way of knowing for sure exactly how far the criminal activities went in this case; is that correct?

MR. IAVARONE: That is correct.

MR. LIPMAN: It is also not clear in Illinois, talking about corroboration—even if this gentleman would cooperate fully, you still would have no corroboration of criminal activity on the part of the third person, whereas, if you had a wiretap, the voice of the third person would be enough corroboration?

MR. IAVARONE: That is why I say the opportunity was missed.

MR. LIPMAN: I have no further questions, Mr. Chairman.

MR. REMINGTON: Judge Shientag.

MS. SHIENTAG: Mr. Gillis, with your broad experience both as a defense attorney and a prosecutor before and now, you are singularly equipped, it seems to me, to provide us with information, and especially since you have expressed a very fine understanding of the balance of Fourth Amendment rights with the needs of the prosecutor to prosecute for crime.

Now, dealing with the safeguards that now exist that didn't when you were first an attorney prosecuting—and I assume that was with the District Attorney's office rather than in the Federal sector; right?

MR. GILLIS: Yes.

MS. SHIENTAG: Name some of the safeguards that you find particularly helpful to defendants at the present time.

MR. GILLIS: Well, I think we have to be careful that non-criminal conversations are not being seized.

MS. SHIENTAG: You are talking about minimization?

MR. GILLIS: Yes. We must be careful that we are using a microscope to gather the type of evidence rather than wide field glasses that take in innocent conduct.

Then, as I alluded to before, I think we should insist on a careful description of crime and probable cause that we are going to obtain valuable evidence, so we don't either invade people's rights or waste the time and utility of the police in gathering evidence that is not going to be fruitful.

MS. SHIENTAG: You are talking particularly about wiretaps, but I wanted to direct your attention to the broad general sphere of the protections that defendants in criminal cases have.

There are many protections, the right to inspect grand jury proceedings, the right of discovery and inspection, and so on?

MR. GILLIS: Yes.

MS. SHIENTAG: And in addition to that, protection against the dirty business of listening in on someone else's conversation, we have the court-ordered requirements of probable cause before you get an order, and limitation of time, and sealing, and an inventory, and the defendant provided with all the information that has been taken against him.

Now, have you ever had wiretapping under court order in your jurisdiction?

MR. GILLIS: No.

MS. SHIENTAG: Have there ever been any attempts to put that into the legislation?

MR. GILLIS: We have not moved in that direction because of the evaluation that the political mood was such that it would be greeted by a move in the opposite direction. In fact, that is the way our Legislature is going.

MS. SHIENTAG: By "the opposite direction," you mean a limitation of the consensual wiretapping?

MR. GILLIS: Yes.

MS. SHIENTAG: When was the act you referred to permitting consensual wiretapping enacted?

MR. GILLIS: In. 1961.

MS. SHIENTAG: Prior to the Omnibus Crime Control Act?

MR. GILLIS: Yes.

MS. SHIENTAG: So you have not had non-consensual wiretapping prior to 1968, either?

MR. GILLIS: That is correct.

MS. SHIENTAG: And has there been an attempt to erode the 1961 Act, to limit it? I think you said you submitted a bill to the committee?

MR. GILLIS: Yes. In this session of the Legislature—and perhaps United States Attorney James Thompson can amplify some of the motives behind this—it might just incidentally have something to do with a case made by Jim Thompson against some members of the Illinois State Legislature—I am not sure that is true. But this year a bill has been enacted that severely limits our power to consensual overhear.

MS. SHIENTAG: It has not been enacted yet, though?

MR. GILLIS: It has not been enacted, but it has passed the Illinois House. And I think the bill presents a danger to sincere law enforcement in the State of Illinois and I have expressed that view to the Legislature, at this point without success.

MS. SHIENTAG: You don't hope to have a general wiretapping act similar to the Federal one in your state?

MR. GILLIS: Politically at this time I don't harbor that as a realistic hope in the State of Illinois.

MS. SHIENTAG: What you hope for is that the consensual one not be taken away?

MR. GILLIS: That is right. I would like to preserve the status quo.

MS. SHIENTAG: And you feel you can operate pretty well under the present law?

MR. GILLIS: That is right. I think what we have is a very effective law enforcement tool. As we have said, we have seen instances where non-consensual wiretapping could be of tremendous aid to the state and the people of the state. In the instance of the stolen goods rings we are dealing with, some of these may be raising costs of certain consumer goods in our country by as much as 5 per cent.

These things hurt every person. Every person that goes to the grocery store is feeling the pinch of this sort of crime. And I think we could stop it if we had the tools.

MS. SHIENTAG: Not only that, but when an investigation is undertaken by a grand jury for the purpose of reaching the higher-ups, you have someone testifying as to what has happened and the area of motivation and so on creeps into his testimony.

As opposed to that, you have electronic surveillance—and I am speaking of non-consensual as well as consensual. You have evidence of an ongoing crime. You have the words, themselves, of the criminal coming forth in the course of the trial, which is more subject to being fruitful.

MR. GILLIS: If I could interrupt there, we could stop serious crime. There is a criminal market in the county for, quote, "clean weapons," weapons without ballistics marks to be used in sophisticated, large-amount armed robberies. And we know the route that is followed to gain those weapons. It is a phone in a particular tavern.

With that information partially corroborated, we know exact how it works.

If we could have a legal non-consensual wiretap of that phone we could find out when guns were being ordered for a criminal enterprise and who was going to be picking them up. We could stop crime before it happened just as could have prevented Purolator.

MS. SHIENTAG: So your hands are tied by the limitations of investigation along this arm of the law?

MR. GILLIS: Yes.

MS. SHIENTAG: Now, with regard to the Purolator case, why didn't you bring the FBI in? They are not restricted. And here you had goods moving in interstate commerce.

MR. GILLIS: Well, we did notify the FBI, but insofar as the Purolator evidence, it did not appear there was Federal jurisdiction at an early stage. It turned out later that Purolator is insured and as such is legally a Federal bank. But at the time we had only the broad, hazy description of it so the FBI at that time ruled they did not have jurisdiction.

MS. SHIENTAG: They determined that?

MR. GILLIS: Yes.

MS. SHIENTAG: Let me ask you just one question about the statement you submitted to the Commission. This says, "Having been duly advised of the circumstances, I hereby grant consent for the person to either tap a wire or carry a body recorder."

In the Purolator case, for example, would that be done every day?

MR. GILLIS: It would be done perhaps every day. The broadest period of time would be every three days.

MS. SHIENTAG: So every time you wanted to give a receipt, you would have to listen to what had been discovered the day before?

MR. GILLIS: Uh-huh.

MS. SHIENTAG: Then a considerable part of your work day would be occupied with just reviewing that one agent's testimony?

MR. GILLIS: Yes, it would, but sometimes we would relate to the State's Attorney, "This involves confidential investigation in a certain number" and he would say "Oh, yes," and we would say "We talked to you about that three days ago" and he would say "Oh, yes." So it moves along and it is not that restrictive.

MS. SHIENTAG: So this is a restriction you imposed upon yourself?

MR. GILLIS: Yes.

MS. SHIENTAG: So, summing up your experience as a defense attorney as well as a prosecutor, would you say rights of defendants are adequately protected under consensual wiretapping as it exists now?

MR. GILLIS: Yes, I do. I think we have a marvelous government, a government that has confidence in its people. It builds in these protections because it has confidence in its own stability and its own worth. And I think we have had adequate protections to protect the person accused of crime.

As so often said—the words might sound trite, but I sincerely believe them—the average citizen also needs protection.

MS. SHIENTAG: Why do you suppose people are so afraid of being listened to?

MR. GILLIS: I am thinking of the Chairman's quandary over that problem. I suppose there is some aspect of the newness, comparative newness, of electronic evidence. And as the year of George Orwell's book approaches, maybe we all recall the horrors that he described.

But I sincerely think there is a certain area of our citizenry that are harassed by arrest and search, but the people that feel most threatened are not that economic segment. We are dealing with ourselves here.

MS. SHIENTAG: They are being harassed without electronic surveillance?

MR. GILLIS: Yes. I presume there would be more trouble, as most people think about it, by arrest or search of their whole house, apartment, and things of that nature.

But we are dealing here in many areas with crimes of bribery, official corruption, and these things are reflected by the people who are most concerned about them.

I guess I am not making myself too clear.

MS. SHIENTAG: You made a remark before that the ones concerned with bribery might be the very ones who might be in a position to restrict your present consensual electronic surveillance law. Did I understand you correctly?

MR. GILLIS: Yes. And I think it is important that all legislative chambers and judicial chambers be free to do the job that they were intended to do. I think they should be sanctuaries for the protection of those elected to these positions of trust to go about their work in an atmosphere of confidence.

But I think there is an over-concern by certain legislators because, frankly, they feel they might be the target for this sort of evidence.

And at the same time we find no bills in to have reports about their execution of search warrants, because the legislators feel no personal fear for that use of power.

It seems to me a question of whose ox is being gored and the concerns are ripest that are close to your door.

MS. SHIENTAG: They have something to conceal, you are implying?

MR. GILLIS: I think that is the way they feel. I don't know if they have anything to conceal or not, but apparently they exhibit some disproportionate amount of fear about this sort of evidence if they have nothing to hide.

MS. SHIENTAG: Thank you very much, Mr. Gillis.

Thank you, Mr. Chairman.

MR. REMINGTON: Mr. Blakey?

PROFESSOR BLAKEY: What time are we going to break for lunch?

MR. REMINGTON: Very soon. I was going to ask whether Mr. Gillis and Mr. Iavarone would be able to come back after lunch. Chief Andersen, who had a conflict, told me he hoped to have an opportunity to ask you a question or two.

PROFESSOR BLAKEY: Do you have an early airplane reservation?

MR. GILLIS: No, it's about four o'clock.

MR. REMINGTON: Why don't we recess for lunch and see if we can reconvene at about 1:30.

[Whereupon, at 12:30 p.m., a luncheon recess was taken until 1:30 p.m.]

AFTERNOON SESSION

MR. REMINGTON: I think we are ready to reconvene.

I understand Lieutenant McFadden is here and has been waiting patiently.

I appreciate your coming, Lieutenant.

As you know, the rules of the Commission require that you be sworn.

[Whereupon, Lt. Daniel McFadden was duly sworn by the Chairman pro tem.]

TESTIMONY OF LT. DANIEL McFADDEN, COMMANDING OFFICER, ORGANIZED CRIME UNIT, PHILADELPHIA POLICE DEPARTMENT

MR. REMINGTON: We are sorry we kept you waiting this morning. I know we have a prepared statement, and without objection that will be made part of the record.

Do you desire to start with the statement?

LT. McFADDEN: If you would like me to read it, I will, sir.

Mr. Chairman, I am Lt. Daniel McFadden, Commanding Officer of the Organized Crime Unit, Philadelphia Police Department.

One of my responsibilities is intelligence gathering on organized crime figures and the dissemination of this information to all agencies. I am also the liaison officer for the Police Department with Federal, state and local agencies dealing in organized crime. I would like to direct my first remarks to wiretapping and inform you that this is not permissible in Pennsylvania by state or local law enforcement officers.

It is believed that, in the Philadelphia area, gamblers know that we, as law enforcement officers, are forbidden to wiretap and, thus, they conduct most of their illegal activities over the telephone. They have no fear of the local police breaking the law by wiretapping, and this enables them to go about their illegal activities in comfort in their secure hiding places. I have personally seen places that are constructed solely for gambling purposes; these are equipped with double and triple steel doors which are barricaded.

In the Philadelphia area we suspect that approximately 85 per cent of all illegal bets are taken over the telephone. This is accomplished by persons working the "office" who call the number writer at a given time, and accept the bets. This office person will call as many as 15 or 20 writers.

The reason for the office person calling is that the number writer, himself, does not know where this office is located. Investigations have indicated that a banker could have as many as ten of these offices located throughout the city. This minimizes his risk of losing the majority of his action for the day in the event of a police raid.

Recently it has been found that bankers are recruiting housewives, with no criminal record, to man these telephones in their own homes and paying them \$50 a week for working a maximum of three hours a day. As you can see, this again minimizes the risk of having the work confiscated.

There is no way of knowing how large an organized crime figure is without the use of a wiretap. He might be engaged in illegal lottery, horse and sports betting, loansharking and other illegal activities, and remain unknown to police under our present law in Pennsylvania.

Wiretapping, as well as electronic surveillance, could be abused by anyone without the proper controls. The best safeguard to combat this would be the careful selection of personnel who would use these aids. One of the most important qualities would be integrity of the individual and of the unit to which he is assigned. The key ingredient would be to uphold the law while enforcing the law.

We must realize that, under the restrictions in Pennsylvania, we in law enforcement are hampered in doing our job, and we cannot intelligently identify all members of an organization, or the scope of their illegal activities, without the use of this investigative aid, wiretapping.

The second topic of discussion: Non-consensual electronic surveillance. House Bill 1588 was passed on October 2, 1974 in the State of Pennsylvania amending Title 18, "Crime of Eavesdropping." This amendment is entitled "Invasion of Privacy." In brief, we in law enforcement are not permitted to conduct any type of recording without the approval of all persons being recorded. There are three exceptions:

1. Personnel of a telephone or telegraph company in the performance of their duty.
2. The President of the United States or those acting upon his direction.
3. Duly appointed state or local law enforcement officers, only under one condition. "This exception shall be limited to those situations in which the personal safety of such law enforcement officers is in jeopardy and shall not include any right of recordation."

I will direct my remarks to the third exception.

This exception must be court approved by first making application through the District Attorney's office, who must approve it, and then be taken to a judge of a court of record. This, of course, is very time consuming. The District Attorney and the judge would be available for approximately eight hours of the day; as you can well realize, police can be in danger 24 hours a day.

On many occasions an undercover police officer is out of the vision of a backup team, and a transmitting device is the only contact with outside help.

When an investigation is under way, situations can change in a moment's time which could endanger the investigating officer, and it would be impossible to obtain a court order under these conditions.

In my humble opinion this law protects only the lawbreaker and not the law enforcer.

If I may, I would like to relate a few occasions in which I personally was involved and you consider the hindrance to law enforcement.

On one occasion my office was contacted by the Pennsylvania State Police requesting assistance in a narcotics investigation where one of their undercover officers was coming into the city to make a buy, but he did not know where the transaction would take place. He was to be accompanied by a known drug user who was not trusted by the state police. There was to be a 2-ounce cocaine buy.

The undercover agent, along with a state police back-up team, came to my office, and we immediately put a body transmitter on the undercover agent which enabled us to have continuous communication from him. Three different automobiles were used to surveil the undercover officer. A signal system was set up so that, in the event the undercover officer said, "This looks like dynamite," we knew the purchase was made.

It so happened that this transaction took place in Center City at a busy intersection in a four-story building. The undercover officer was out of the sight of the surveillance teams.

I monitored the receiver and when I heard "This looks like dynamite," a signal was given to all teams to move into the building. As we were approaching, the undercover officer stated, "The girl is throwing the coke out the window." This enabled us to stand on the pavement and recover the two ounces of cocaine.

He also gave us directions to the exact location of the apartment. The main subject ran from the room stating he was going to get a gun. The transmitter enabled the undercover officer to warn the backup team that the subject might have a gun. Of course, this required us to break in the door for the safety of the undercover officer.

The successful outcome of this case resulted in three persons arrested, confiscation of the cocaine, and, most important, no harm came to the undercover state police officer.

I would like to point out that this particular investigation took place on Saturday morning; the arrangements for the buy were made late Friday night in a town located about 45 miles from Philadelphia. Under our present law, it would be impossible to obtain a court order in time to make this aid available for our use.

Another case came to my attention when two Philadelphia police officers contacted our office and requested one of our surveillance cars as they had made a contact to buy one pound of speed for the sum of \$7,000. I inquired as to their need for

our surveillance car on this particular assignment. Their answer was that the buy was going to be made from a "flashy" girl and she would be impressed by a large car. After questioning, I discovered I was familiar with this female's background as she had an extensive criminal record with 11 arrests. The officers were cautioned and their commanding officer was apprised of this person. He requested that I guide his men.

The transaction was to take place at nine o'clock that evening in front of a South Philadelphia motel. I ordered the car to be equipped with a transmitter and had the door rigged on the right-hand side so that it could not be opened without the officer disengaging the lock. Also, this surveillance was video-taped.

It turned out that the decision made was a proper one. The transaction took place inside the vehicle; however, this "flashy" girl had other things in mind. She attempted to get out of the vehicle with the money and, at that time, it was planned that two men would hold up the police officer for the drugs he had just purchased.

This investigation resulted in three persons being arrested, one pound of meth and a 9 MM automatic confiscated, and, again, most important, no injury to the police officer.

Another example took place at 10:00 P.M. on a week day. I was contacted at home and informed that a narcotics raid had taken place; confiscated were drugs and what appeared to be loansharking records.

I was informed of the defendant who was known to me to be a enforcer for loansharking. Being aware of the syndicate for which he worked I advised the officers that, in all probability, an attempt would be made to purchase a copy of these records.

When I arrived at narcotics headquarters, the police officer was on the phone with an unknown person who stated, "We will make it worth your while to copy the papers."

I suggested that a meeting take place within an hour and a half of the time of the phone call. I ordered a body transmitter to be placed on the officer prior to this meeting.

Within two hours this meeting took place inside the manager's office of a well-known hotel in Center City, where the manager, who is a brother of a prominent attorney in Philadelphia, offered the officer \$500, which he paid to the officer. At this time, he was promptly arrested.

It turned out that the manager was carrying a gun on his person.

With the aid of the body transmitter, three different police officers heard the manager of a large hotel bribe a single police officer.

These related incidents are given to you to show the importance of the time element and the restrictions placed on law enforcement. It is my belief that if the legislative body in Harrisburg was aware of the dangers experienced by police officers in the performance of their duty, this restrictive law would not have been passed.

Thank you for your attention.

MR. STEIN: Thank you, Lt. McFadden.

Lieutenant, can you outline your own background and experience in law enforcement?

LT. McFADDEN: Yes. I have been in the police department for 19 years. I worked patrol for two and a half years. I worked the Vice Squad for a year and a half. I worked the narcotics unit for three years. I was promoted to Detective. I worked on special assignments to the Chief Inspector of Detectives.

When the Organized Crime Unit was formed, I was assigned to it. And I worked as the Administrative Aide to the Chief Inspector, and I have been the Commanding Officer of the Organized Crime Unit for the last three and a half years.

MR. STEIN: Can you describe the nature of the Organized Crime Unit and its mission?

LT. McFADDEN: Yes. We are an intelligence-gathering agency for the Philadelphia Police Department, and one of our main jobs is to cooperate with all law enforcement agencies in the battle against organized crime.

MR. STEIN: Can you outline the intelligence efforts that your unit makes—the nature of its work and the methods of its investigation?

LT. McFADDEN: Our unit makes no arrests. We surveil. We gather information through other agencies that assist us. We try to take the investigation as far as we can without revealing ourselves, and then we turn it over to whoever can do the best job in prosecution.

MR. STEIN: Your unit is directed toward organized criminal activity in Philadelphia?

LT. McFADDEN: That is correct.

MR. STEIN: In narcotics, too?

LT. McFADDEN: Narcotics activity, also.

MR. STEIN: Can you describe any of the other types of activity that your unit engages in?

LT. McFADDEN: Of course the gambling, horse bets, numbers, loansharking—actually, all the crimes that would need an organization. We are also now trying to get into labor a little bit.

MR. STEIN: You cooperate with Federal authorities and at some point in your investigation you have turned over information to Federal authorities for further investigative efforts. Is that correct?

LT. McFADDEN: That is correct, sir.

MR. STEIN: Can you outline some of the criteria that make you decide to turn a case over to Federal authorities rather than to continue with it in the Philadelphia Police force?

LT. McFADDEN: Of course, as we are saying here today, we don't have wiretapping. And we will come across information that a person is getting exceptionally large in the gambling area, or the narcotics area. And our hands are tied due to the fact that everything is done over the phone in Philadelphia. They have no fear of it whatsoever.

At this time we will go to the FBI and request that they look into it and hopefully they do, and on occasions they have.

MR. STEIN: To your knowledge have any successful Federal investigations resulted from information you have turned over to the FBI?

LT. McFADDEN: Yes.

MR. STEIN: In what kind of activity?

LT. McFADDEN: In the activity turned over to the FBI it would be gambling. We have created interest with DEA in narcotics and we hope that we have spurred certain things on that enabled them to go after a court-ordered Title III and secure a wiretap.

MR. STEIN: On the other hand, your division or the Philadelphia Police generally do not accept information from wiretaps in other jurisdictions?

LT. McFADDEN: That is correct.

MR. STEIN: What do you do if you have information coming off a legal Federal tap or a tap in a neighboring jurisdiction that a murder or some other major criminal activity is going to take place in Philadelphia?

LT. McFADDEN: What would I legally do or what would I do?

MR. STEIN: What action would you take?

LT. McFADDEN: I would take action.

MR. STEIN: Specifically, the Commission has been told about a case arising from information received in New Jersey of an arson being planned in Philadelphia. Do you know anything about that case?

LT. McFADDEN: Yes.

MR. STEIN: Can you tell us what role the Philadelphia Police played in that?

LT. McFADDEN: We have a fine and good working relationship with the New Jersey Organized Crime Units. And on a Saturday afternoon they called me at home to verify if a certain fire was taking place. I verified it for them and they called back—or I called them back and I verified there was a fire. And they informed me that it was not a fire; it was a fire bombing.

And here it so happened that they, the New Jersey State Police, were tailing them over from New

Jersey and they also wanted to notify me that they were in the city. That is our agreement that anytime they come into the city they notify me.

MR. STEIN: And the Philadelphia Police will be able to help in a protective role and an investigative role in a situation like that but they will not be able to make the arrests in the case?

LT. McFADDEN: In the case of the firebombing?

MR. STEIN: In the arson case.

LT. McFADDEN: I was requested to go over to New Jersey after they were placed under arrest, which I did. I brought a detective assigned to the arson unit with me.

At that time the FBI and the New Jersey State Police were going to prosecute first. As far as the arson prosecution in Philadelphia, I have no knowledge of that yet.

MR. STEIN: One of the problems raised in Philadelphia and some other jurisdictions, especially towards gambling, but perhaps more generally, is that sentences are not very effective in Philadelphia; there are problems to convene an investigative grand jury. In other words, more ordinary and normal processes of investigation than wiretapping themselves are not used effectively in Pennsylvania.

Is that a particular problem? Specifically, if you had wiretapping authority in gambling cases, considering that sentences in gambling are very minimal in the Philadelphia area, what good would it do you in fighting organized crime?

LT. McFADDEN: The main thing, as I pointed out in my statement, is there is no way that anyone can tell how large an organization is unless you have, in my opinion, wiretapping in gambling. Because, as I also stated, they have absolutely no fear of doing all their talking, making all their contacts, and I feel that if the court system would see how large and how widespread it is, I think you might see some tougher sentences.

MR. STEIN: Do you know the outcome of the Federal cases in which gambling convictions were obtained?

LT. McFADDEN: The outcome in Federal cases? Now, in the Philadelphia area the Federal judges, I know—most of them are fined and put on probation. And this type of people, if they are what I would feel higher-ups in organized crime, we take a physical or a visual surveillance of them as much as we can to see if they are back in business. And if they are back in business, I will set up the arrest and I will notify the FBI that someone is in violation of his probation. We had one case approximately a month ago where someone was sentenced to four years in prison for violating his probation.

MR. STEIN: Do you agree generally that there are difficulties in effective sentencing in the Philadelphia courts and in other aspects of the criminal justice system?

LT. McFADDEN: In gambling cases?

MR. STEIN: Yes, or even in narcotics.

LT. McFADDEN: My personal opinion? I think they are ridiculous. All the time, the money, and effort spent, and they might get \$150 or \$500 fine and that's it. They are not even put on probation. Within, I would say, five months they are back in business.

MR. STEIN: Do you have reason to believe there is extensive narcotics activity in the city?

LT. McFADDEN: When I was in the Philadelphia Narcotics Unit—I was in there for three years—there were 18 men assigned to the entire city of Philadelphia. And we had to go around searching for arrests. Today there is an excess of 80 men and they are overworked. There is a big problem, in my opinion.

MR. STEIN: One question we might direct to you: All non-consensual wiretapping statutes require the approval of the local prosecutor prior to obtaining a court order, the idea being presumably that the police should have the legal guidance of the prosecutor at all times.

Do you believe a system like that is necessary and workable in Philadelphia?

LT. McFADDEN: I believe everyone should have control. It would have to be the District Attorney's Office, yes, but not necessarily so.

MR. STEIN: Do you believe the police, then, should, themselves, exercise wiretapping authority and investigative authority at all stages prior to the indictment or arrest?

LT. McFADDEN: Well, of course we can't wiretap. We can't wear a body device. So it is—I really can't answer that. If you are asking for controls, I would say there should be very strong controls. But again, as I pointed out, it is not what controls are put on but the people, themselves, that are actually operating it. I think that is more important.

MR. STEIN: Last but not least, can you tell the Commission what has happened in Philadelphia since the beginning of this year when the police were not allowed to use non-consensual electronic surveillance any longer without a court order, and even with a court order you can only use it for protection. What has happened in the kinds of emergency situations that you have outlined in your statement?

LT. McFADDEN: I can give you one example. Again the Pennsylvania State Police came to me to make a narcotic buy and we felt we knew exactly where the buy was going to go down, so that was

easy. We covered it. The State Police officer got in the car with the informant—he wasn't an informant; he was the guy who was going to make the buy. And there is a standard rule in our department that any time that you expect or anticipate trouble, we notify a stake-out unit. They are uniformed personnel, experts with firearms. I did that. It took us six cars to follow the guy all over the City of Philadelphia and where I had all the cars lined up in West Philadelphia, we ended up on the 5200 block of North Broad Street, which is pretty far up in North Philadelphia.

And time, effort, and the worst thing about it was we lost the police officer once.

MR. STEIN: You lost him when you tried to follow him?

LT. McFADDEN: Right. And when he went into the apartment and made the buy, we didn't see him. When he came back out he had talked to the man he had just brought the stuff from hoping we were there. When we went back and searched that particular apartment it had four guns in it and they had two particular apartments they were working out of which we had no knowledge of. We lost visual sight of him completely and I felt very strongly about it because here was a visiting police officer coming in and asking for my help and I goofed it.

MR. STEIN: You try to protect your police officer now by physical surveillance?

LT. McFADDEN: The only way we can do it.

MR. STEIN: In an emergency situation you merely use physical surveillance then?

LT. McFADDEN: Yes, we do. We have these high-rise apartments which I have done also. The Pennsylvania State Police came in and were going to make a purchase and it was a high-rise apartment and I told them, "Call it off; forget it. It is not worth it."

MR. STEIN: What do you do if you have an informant tell you of a narcotics transaction or some other criminal transaction and he is a new informant or someone who is not reliable? What steps can you take to corroborate his information?

LT. McFADDEN: Well, that would be another physical surveillance type thing, to watch him. I normally don't run into those situations in checking out informants.

MR. STEIN: Okay, that is the staff questioning, Mr. Chairman.

MR. REMINGTON: Mr. Blakey.

PROFESSOR BLAKEY: Lieutenant, in 1974 there was an extensive investigation of the Philadelphia Police Department by the Pennsylvania Crime Commission and it indicated, frankly, more corruption than most people would like to associate with a major metropolitan department.

Without asking you to comment directly on the conclusions in that report, do you think that the Department or the other law enforcement agencies in the City of Philadelphia can make an adequate response to the problem of police corruption without, at a minimum, consensuals?

LT. McFADDEN: Without what, sir?

PROFESSOR BLAKEY: Without, as a minimum, the ability to use consensuals?

LT. McFADDEN: The Pennsylvania Crime Commission did report that we had widespread corruption. At that time I was in command of the Organized Crime Unit. I still held my good faith with the FBI, with the Pennsylvania State Police, with the New Jersey State Police, with DEA, Internal Revenue Service. It didn't faze us one bit.

PROFESSOR BLAKEY: No, I am not raising with you the level of cooperation between your unit and the others. I am familiar with the testimony that was given before the National Gambling Commission in which the FBI indicated that indeed they did not have problems in dealing with your unit, that the corruption indicated to be present in the Philadelphia Police Department did not involve you or your unit.

My question was directed to: Do you think the law enforcement agencies in Philadelphia—I am referring particularly to your own internal investigations unit, the Philadelphia District Attorney's Office, the State Attorney General's office, or anyone else—could respond to the problem of police corruption in Philadelphia unless they had the power to record bribery situations?

LT. McFADDEN: I would say they would have to have the power to record it, because normally when something like that is done it is done on one-on-one person and you have no corroboration.

PROFESSOR BLAKEY: So in a sense, when the State Legislature enacted the new statute they kind of gave a license to steal to corrupt police officers, corrupt legislators, corrupt prosecutors, or corrupt judges, because now they are insulated from effective means of investigation? Is that correct?

LT. McFADDEN: I wouldn't say a license to steal, no sir.

PROFESSOR BLAKEY: Well, at least a license to avoid the normal investigative processes that are most effective in dealing with corruption.

LT. McFADDEN: It is a very strong tool in the investigation, but I would not go out and say license, no.

PROFESSOR BLAKEY: I have no further questions.

MR REMINGTON: Judge Shientag?

MS. SHIENTAG: No questions; thank you.

MR. REMINGTON: Chief Andersen?

CHIEF ANDERSEN: I have one question. I am sorry I was late. Your law of invasion of privacy on your consensual recording: How do you handle just routine interviews of people or taking of statements under this law?

LT. McFADDEN: A secretary.

CHIEF ANDERSEN: You have no way, then—you are forbidden, then, just on a routine interview of a person, to record?

LT. McFADDEN: If we have their full permission, both parties knowing a recording is being made, we can do it.

CHIEF ANDERSEN: On a routine burglary pick-up, a routine crime pick-up, a routine interview, you can't record?

LT. McFADDEN: No, sir, unless the other person agrees.

CHIEF ANDERSEN: You wouldn't want to throw that in with *Miranda* warnings, too, but you would have to if you were planning on using recording, just routinely interviewing?

LT. McFADDEN: Yes, sir.

CHIEF ANDERSEN: That would be quite a handicap, I would think.

LT. McFADDEN: It is quite a handicap.

CHIEF ANDERSEN: In the police stations, do they record the incoming calls for services?

LT. McFADDEN: The tape recording?

CHIEF ANDERSEN: Yes.

LT. McFADDEN: Yes, they do. They do it with a beep.

CHIEF ANDERSEN: Wouldn't that be illegal here?

LT. McFADDEN: No. I believe—I believe, now—that what did raise a question at the time of the Crime Commission was there was a prosecution of a newspaper reporter in the Philadelphia area, and he recorded. And that is what he brought up as his defense, the police department reports all incoming phone calls to the radio room. And if you call the police department radio now you will get the beep, I think it is every 15 seconds or something like that. And this, they say, is notification that you are being recorded.

CHIEF ANDERSEN: But the beeping does not clear you from the state statute as I am reading this paper. I am not trying to put you on the spot, Lieutenant.

LT. McFADDEN: Legally, I can't answer it. I know that was an argument in a case approximately three years ago, and the beep apparently satisfied the courts.

CHIEF ANDERSEN: A further question: Do you record your radio conversations between your radio cars in Central Station?

LT. McFADDEN: Yes.

CHIEF ANDERSEN: Do you have the approval of all the policemen in Philadelphia?

LT. McFADDEN: I am pretty sure there is approval. If you ride in a police car you had better have approval.

CHIEF ANDERSEN: You see what I am getting at. I am talking about the routine policing side which seems to be covered by this law and I question whether they had any intentions of doing that. But I am reading it as they completely shut you off from even recording communications between radio cars unless you have the approval of all persons being recorded.

LT. McFADDEN: Well, it is a known fact that tape is running 24 hours a day. And of course that is done mainly for investigative purposes. The time is recorded automatically on the tape.

CHIEF ANDERSEN: I appreciate the fact and it is very important when somebody calls the Philadelphia Police and says "I have just been stuck up"—time becomes critical later on in the case. And that is very true. But I read this that you are in conflict.

LT. McFADDEN: That is the only thing I can say—that beep was supposed to satisfy it.

CHIEF ANDERSEN: That was supposed to satisfy it?

LT. McFADDEN: Yes.

CHIEF ANDERSEN: I have no further questions.

PROFESSOR BLAKEY: Lieutenant, would you explain to us why the police record all incoming calls on emergency numbers?

LT. McFADDEN: I cannot give you the official Police Department—

PROFESSOR BLAKEY: Just the practical reasons.

LT. McFADDEN: It is a great investigative aid for, as we said, the time element, which is number one. The second is the exact wording the people used.

As you know, in a hold-up situation or a shooting situation, a lot of times people will get on there and they will be just rattling off and it is not clear.

PROFESSOR BLAKEY: Do they ever hang up before they are finished?

LT. McFADDEN: A lot of times they do.

PROFESSOR BLAKEY: And the only way you can find out what they said is replay the tape?

LT. McFADDEN: I saw that done many times, yes, in very serious cases, yes. What we try to do is hold them on the telephone and as the police officer is talking it will go over the police radio, so there is no lapse of time whatsoever. And I do know—

PROFESSOR BLAKEY: Do you think there would be any problem, if every time an emergency

call came in the emergency operator said, "Before you say anything else I have to tell you this call is being recorded."

LT. McFADDEN: No, but if you hear this beep—this is what I understand. I heard people interviewed over the radio from a telephone and they are getting the same beep that the police radio gets and no one is complaining.

PROFESSOR BLAKEY: I have no further questions.

CHIEF ANDERSEN: I have no further questions, Mr. Chairman.

MS. SHIENTAG: I just wanted to ask the question: With regard to what the Chief was asking you about, isn't it true that the law prohibits the use in court of recordings from consensual wiretapping, what we term consensual wiretapping? He was talking about an investigative procedure in the police car, and that wouldn't necessarily resolve itself in a case where such evidence would not be permissible.

In other words, I am trying to clarify the question. I may be casting more confusion on it.

The Chief was asking you about the recordings that are made in the course of police duty, so that you know when a crime has been committed and so forth.

LT. McFADDEN: Right.

MS. SHIENTAG: Now that isn't looking toward the investigation of another crime that you are going to present. That is for the clarification of the administrative procedure in your office, isn't that right?

LT. McFADDEN: That is administrative procedure, yes.

MS. SHIENTAG: So that you will know and be able to investigate further, rather than to use that particular recording as evidence at court?

LT. McFADDEN: Oh, that is not the reason for it.

MS. SHIENTAG: I thought that might clarify it.

LT. McFADDEN: I'm sorry. I thought you asked two questions. One was the recording of police radio—

CHIEF ANDERSEN: Yes.

LT. McFADDEN: And the other in the investigative stage where we would interview a particular person.

CHIEF ANDERSEN: I was talking from three standpoints, probably. One is the "call for services" recording and the second is the police car recording. But I am looking at the routine bugging, if you want to use that term, of an interview room, just almost routine policing. If you interview somebody, you record it. This is both for the benefit of the officer doing the interrogating and the person, and the office, and it is routine in police work and yet you are prohibited.

LT. McFADDEN: That is right.

CHIEF ANDERSEN: So when your officers go into the interrogation room you have no idea of what is going on unless you sat in as an administrator?

LT. McFADDEN: It would be a situation where you would take two people in with you?

CHIEF ANDERSEN: Yes.

LT. McFADDEN: We are not allowed to do it.

MR. REMINGTON: Lieutenant, thank you very much. You have been very helpful and we appreciate your coming.

LT. McFADDEN: Thank you, sir.

MR. REMINGTON: Neither Professor Blakey nor Chief Andersen had an opportunity to pursue their questions with Mr. Gillis and Mr. Iavarone and we would like to do that.

Mr. Thompson and Mr. Phillips are also here.

FURTHER TESTIMONY OF KENNETH L. GILLIS AND NICHOLAS IAVARONE

MR. REMINGTON: I think we have gotten as far as asking you whether you have questions.

PROFESSOR BLAKEY: Mr. Gillis, about how many requests for consensuals do you process in a week?

MR. GILLIS: I would say on the average of about five a week.

PROFESSOR BLAKEY: Do you have any provision in your state statute for emergency consensuals? In a situation where the police officer simply could not find the State's Attorney, what would he do?

MR. GILLIS: No, we have a series of exemptions, one of which covers emergency calls to the police department—Mr. Andersen's question. But we have no general emergency provision in our law as it is now enacted.

PROFESSOR BLAKEY: Does your state statute specifically exempt emergency calls to the police department?

MR. GILLIS: Yes. In the bill that I referred to, H.B. 212, there is an emergency provision which would exempt prior petitioning to a judge for permission. And the description of what is an emergency is not too explicitly drawn up.

PROFESSOR BLAKEY: I am somewhat confused between proposed law and present law.

Under present law in Illinois, where consensuals must be approved by the State's Attorney—

MR. GILLIS: Right.

PROFESSOR BLAKEY: —that does not apply to emergency calls to the police?

MR. GILLIS: There is no emergency provision exempting that procedure, none.

PROFESSOR BLAKEY: There is none?

MR. GILLIS: No.

PROFESSOR BLAKEY: What is the legal status, then, of calls to the police in Chicago?

MR. GILLIS: I'm sorry. I didn't make myself clear. There is none that by-passes the procedure of getting the consent of one of the parties and the State's Attorney. There is a specific provision which exempts routine calls to police departments and other law enforcement agencies, the normal police number.

PROFESSOR BLAKEY: Oh, that is exempted under present law?

MR. GILLIS: Yes.

PROFESSOR BLAKEY: But there is no provision for not emergency calls to police, but emergency situations?

MR. GILLIS: There is no exemption for extraordinary circumstances or danger of the police officer or anything of that nature.

PROFESSOR BLAKEY: In your previous testimony you indicated that in approving consensuals you applied a kind of test of probable cause. Do you mean traditional *Spinelli*-type probable cause?

MR. GILLIS: No, I didn't use it in that term, in the strictness of that expression, but rather in the loose sense of being able to justify what is occurring and what we were hoping to gain.

PROFESSOR BLAKEY: For example, suppose you had a situation where a narcotics buy was going to be made. In a lot of narcotics buys there is a danger to the officer. Would you permit an officer to go in wired where he could not give you information that would tie down the dangers of this particular buy?

MR. GILLIS: Yes, I would.

PROFESSOR BLAKEY: You would put it on a class basis. In narcotics cases as a rule you would permit them even though you couldn't tie the danger to the police officer down to this particular purchase?

MR. GILLIS: Yes. I think that would be a good example.

PROFESSOR BLAKEY: I take it traditional notions of "probable cause" would not permit that kind of "class legislation." It would have to be particularized to the person?

MR. GILLIS: YES.

PROFESSOR BLAKEY: The same thing, say with reliability of an informant. Would you permit a wire to be used to corroborate the reliability of a person you, yourself, did not trust?

MR. GILLIS: Yes. We would not be applying the usual strict standards that go to reliability.

PROFESSOR BLAKEY: If you didn't trust him yourself you couldn't get a search warrant because normally you would have to say that the man, him-

self, is credible as well as his information is credible.

MR. GILLIS: Yes. We would be employing a lesser standard than probable cause, but based on some standard that there would be probability of success.

PROFESSOR BLAKEY: Would you operate on your system of prosecutor approval with the traditional standard of probable cause?

MR. GILLIS: No.

PROFESSOR BLAKEY: In your indication of the kinds of standards that you were applying, as I remember most of them they were seemingly aimed at law enforcement considerations. Do you apply any privacy considerations? For example, would you, all things being equal, permit the recording of lawyer-client conversation, a husband-wife conversation, a doctor-patient conversation?

MR. GILLIS: No, I am particularly sensitive to privileged areas of that type. I think unless you could advance a showing of the importance of such testimony, you would lose more in the privacy area than you would gain in the evidentiary area.

If you could, on the other hand, show a serious crime was occurring and there was some likelihood of gathering evidence at such a privileged meeting, then we would have to assess where the scale would balance. But I would consider the sensitivity of those relationships.

PROFESSOR BLAKEY: So it is fair to say that in testing the propriety of the use of this equipment, you are balancing law enforcement against privacy—you are not just examining whether it is effective for law enforcement?

MR. GILLIS: I am balancing; yes.

PROFESSOR BLAKEY: Do you have any similar policy administratively in supervising police physical surveillance as opposed to electronic surveillance?

MR. GILLIS: I don't supervise the police but if I were advising them I would advise similar considerations in terms of use of their time and the value of the evidence that they recover.

PROFESSOR BLAKEY: Do you think the policy also should have to get a prosecutor warrant to conduct a tail?

MR. GILLIS: I don't know if I would go that far but I think in consideration of proper administration of the police that a supervisor would inquire of the value of surveilling or infiltrating a certain type of organization.

PROFESSOR BLAKEY: I can see this as an administrative judgment by the Sergeant, the Captain, or the Lieutenant. I am asking the broader question. There is a certain reason, I take it, in Illinois that makes people believe there should be

prosecutor approval of this particular kind of surveillance. I am asking you if you think there should be prosecutor approval of physical surveillance?

MR. GILLIS: I am not dodging the question but I think there should be accountability to somebody. And I think it is wrong when a surveillance group or somebody works autonomously. And I think that would be a proper suggestion, to have accountability to a prominent law enforcement official such as the State's Attorney, yes.

PROFESSOR BLAKEY: Would you say the same thing about photographic surveillance?

MR. GILLIS: I don't see the similarity. I have read the articles about the advancing technology—

PROFESSOR BLAKEY: What I am trying to get at is: If we are worried about privacy here, isn't privacy as easily invaded by physical surveillance, by photographic surveillance—I am speaking now in public areas, not in the home. Why should we have these special restrictions on electronic surveillance and not have special restrictions on physical or photographic surveillance?

MR. GILLIS: It is a judgment.

PROFESSOR BLAKEY: What is it about recording someone's voice that makes all the difference?

MR. GILLIS: Well, I don't really see the difference, as your questions point out. But I think what is grouped under the heading "Right to privacy" does more generally describe conversations. There are certain conversations that people feel are private conversations.

PROFESSOR BLAKEY: Do you require prosecutor approval before the police take handwritten notes in conversations?

MR. GILLIS: No. That is right, what you are questioning points out that the law is not exactly logical in this area. If a person had a perfect ear and could commit to paper the conversation he heard exactly perfectly and could communicate it with tone of voice and the rest, it would be exactly the same thing.

PROFESSOR BLAKEY: Let me give you a law professor's hypothetical situation.

Suppose in a police interrogation room you put up a paper-thin wall, had interrogation take place on the left side and on the right side you put a stenographer and told her to take down, just as we are having taken down here, every word that is said.

Would that be any more an invasion of privacy than if the policeman, himself, turned on something?

MR. GILLIS: No, sir.

PROFESSOR BLAKEY: Does Your state statute apply to that?

MR. GILLIS: No. The state statute doesn't exactly know what it is aimed at. There are many instances of overhearing that are not within what the legislature is trying to get at.

PROFESSOR BLAKEY: Let me move on to the Purolator case.

How typical was that investigation of the kind you come across? Or was that an isolated incident?

MR. GILLIS: Well, in scope of the loss it is not typical. But in terms of several persons who make their livelihood from crime I think it is typical, that they are uncovered operating in a certain area, with a certain limited number of telephones. The speed with which they do their criminal buys requires that they use telephones.

And it is typical that if you were able to get an infiltrator into a group of people operating that way, you could uncover detailed plans of their criminal intentions.

PROFESSOR BLAKEY: What I am really asking you is: Sometimes people cite the most difficult and complicated situations.

I am asking you whether the citation of this particular incident is a fair one. Is it typical of a larger one or is it unusual so one can say "That is the exception"?

MR. GILLIS: It is, in terms of any jurisdiction, unusual to have an informant and police undercover agents work into this sort of operation. We started out as a fencing investigation and we ended up with something we didn't anticipate. So it is not typical in terms of "Oh, yes, you are finding this every day."

But what is fair about the example to me is that if you had the imagination and if you had the ability to place informants close to this sort of organized criminal activity, then I think it logical that you could stop crime just exactly as the example shows.

The case, I think, is important for possibilities in law enforcement.

MR. IAVARONE: Let me say that we have one ongoing right now and a smaller-scale one that ended about two months ago, that wasn't that size, but the people were involved in a similar variety of criminal endeavors using a specific telephone.

We started on narcotics as the reason for going in there and it progressed to gambling and stolen goods and guns.

And we have one now. These individuals are not staying in one area but going out, real entrepreneurs, and they are using the telephones to do this.

PROFESSOR BLAKEY: Let me ask you a further question that is suggested by your answer.

Very often the analysis of an electronic surveillance problem has taken place in the context of

thinking about specific crimes: Shall we do it for gambling? Shall we do it for narcotics?

I understand your testimony to say that it is the wrong way to do it, that you are worried about people and the people are engaged in a number of activities and it is the way they engage in those activities that make it vulnerable to electronic surveillance? Consequently, thinking about electronic surveillance in terms of narcotics or gambling is wrong?

I don't want to put words in your mouth.

MR. GILLIS: I guess you are asking about how you sort this out, whether the narcotics people are over here and the gamblers are over here, or contrary to that concept you have cross-disciplinary criminals.

Maybe that is a Chicago breed of criminal operation.

PROFESSOR BLAKEY: Well, how is it in Chicago?

MR. GILLIS: There are large number of people that concentrate in particular criminal enterprises and do not go outside those limits.

PROFESSOR BLAKEY: Do you have a large number of multi-service firms?

MR. GILLIS: Yes, I guess that is what you would call it.

PROFESSOR BLAKEY: Let me ask you one additional question in reference to this last case.

Earlier you or Mr. Iavarone made the point that in these fencing cases it is very difficult to make a case for receipt of stolen property because the goods were not identifiable, and if you didn't have pro-active law enforcement, you wouldn't be able to intervene at times.

I take it, however, if you did have electronic surveillance you would be able to make conspiracy-to-steal or conspiracy-to-fence cases, where you could not identify goods; even though you could not show evidence of actual theft, you could prosecute these cases then, couldn't you?

MR. IAVARONE: Yes, and even with the law we have today, because of the recordings that we would have, the consensual ones with the undercover people, oftentimes we are missing that element of ownership of property. And a lot of our prosecutions then revolve into conspiracy or solicitation.

PROFESSOR BLAKEY: A lot of law professors have worried about whether conspiracy is a necessary crime. Again, I don't want to put words in your mouth, but do I understand your testimony to say in these kinds of investigative situations where you can be sure that a substantive crime has occurred, the practical problems of identification mean the only way they can be prosecuted is through such techniques as conspiracy?

MR. IAVARONE: That, and also if you want to stop the crime before you let it go through to the end.

PROFESSOR BLAKEY: I am talking about after it has occurred.

MR. IAVARONE: Yes, if you don't have that element, I see no other choice.

PROFESSOR BLAKEY: Thank you very much.

MR. REMINGTON: Chief Andersen.

CHIEF ANDERSEN: I have a couple of questions here going into consensuals.

Is there an appeal from the police beyond you on a request for consensual recording?

MR. GILLIS: No.

CHIEF ANDERSEN: There is no appeal for them?

MR. GILLIS: No. Mostly what we do is, if I have a problem with it we talk it out, and we have had no problems along that line. If I communicate to them what I think is missing insofar as what they have, if it is possible to obtain that, we do that. We are not giving them an impenetrable barrier.

CHIEF ANDERSEN: You haven't had any problems?

MR. GILLIS: No.

CHIEF ANDERSEN: Does this law apply to citizens in Illinois?

MR. GILLIS: Yes.

CHIEF ANDERSEN: Can citizens consensually tape any conversation they want?

MR. GILLIS: Now, the law applies to citizens. And to be candid, I think the law, because of its over-breadth in that area, might have some infirmities.

CHIEF ANDERSEN: You mean like a businessman could not tape a contract negotiation under this law?

MR. GILLIS: That is right. It has no provision for common carriers or similar provisions in the Federal law.

CHIEF ANDERSEN: So it doesn't apply to just law enforcement personnel, but literally to the entire State of Illinois?

MR. GILLIS: Yes, that is right.

CHIEF ANDERSEN: I asked this question of the Lieutenant from Philadelphia and ask you the same thing: Do you ever give permission to tape police radio users?

MR. GILLIS: No, our exemption, luckily, handles that so we don't get involved with that.

CHIEF ANDERSEN: It handles all communications between and within law enforcement in general?

MR. GILLIS: Yes. We do get requests from businesses to check quality control procedures of their telephone personnel and things of this nature,

which we have to turn down, even though I think these conversations are governed as they would be in Section 2510 by the conversation that is not intended to be a private conversation. But the Illinois law does not make that distinction.

CHIEF ANDERSEN: And you can't give permission to private citizens, then, to do it at all?

MR. GILLIS: We could, but they would be asking for unlimited amounts of time under tapings of conversations with unknown persons. So, legally, we couldn't comply with that.

CHIEF ANDERSEN: So the same thing applies in Illinois as to law enforcement and the police? In interview rooms they cannot tape just routine interviews of people?

MR. GILLIS: If the tape recorder were open and obvious, I think there would be implied consent, but other than that, they could not.

CHIEF ANDERSEN: On a routine suspect interview they could not just generally tape the conversation without consent from you?

MR. GILLIS: That is right.

CHIEF ANDERSEN: And the answer is, of course, the secretary can sit outside the door and it would be legal for her to take it down in shorthand or by machine?

MR. GILLIS: That is right. It says "by electronic device." If you have good ears, the Illinois law is not particularly concerned about that.

CHIEF ANDERSEN: And one other question. Does the Illinois Bureau of Investigation get their clearance from the State's Attorney?

MR. GILLIS: Yes.

CHIEF ANDERSEN: And they have to go to the individual counties, wherever they happen to be operating at that time?

MR. GILLIS: Yes. There are 102 counties, and of course that presents them with some problems, I would imagine, in certain areas.

CHIEF ANDERSEN: That is all the questions I have, Mr. Chairman, thank you.

MR. REMINGTON: Any other questions?

[No response.]

Well, Mr. Gillis and Mr. Iavarone, I think you will have time to make your four o'clock plane. We appreciate your coming.

MR. GILLIS: Thank you.

MR. REMINGTON: We will next hear from Mr. James Thompson, who we are pleased to have with us. I am sure everyone knows that Mr. Thompson is known for his outstanding record in the field of law enforcement at both the Federal and state level. He is now the United States Attorney for the Northern District of Illinois. Before that time he was First Assistant United States Attorney in that office. Before that time he served at the state and local level,

both as Assistant Attorney General and as Assistant State's Attorney. His career has also been as a member of the faculty at the Northwestern University Law School, co-author of two volumes—all in all very knowledgeable and able and experienced in this field. We certainly look forward to hearing from you.

In accordance with the rules, however, first I will have to swear you.

[Whereupon, James R. Thompson, Jr., was duly sworn by the Chairman pro tem.]

TESTIMONY OF JAMES R. THOMPSON, JR., UNITED STATES ATTORNEY, NORTHERN DISTRICT, ILLINOIS.

MR. REMINGTON: We are certainly glad you could come by. I don't know whether staff has talked to you as to whether you want to start with a statement. The Commission is certainly glad to hear anything you have to tell us.

MR. THOMPSON: Mr. Chairman, first a personal note of thanks for allowing me to change the time of my testimony today. I had a session at the Department of Justice this morning on other matters that took longer than I thought it would.

Secondly, I am pleased to be here today and to meet the Commission, some of them for the first time and some of whom turn out to be old faculty colleagues from the academic world. And, as a former academic person and present case-book author I thank the chairman for the commercial on our criminal law case book!

I thought I ought to speak for a couple of moments today on some fundamental notions on law enforcement that have to do with your work here and be available to the Commission for questions about what we do in Chicago in the areas in which we operate or anything else.

I have watched the criminal justice process in this country all of my professional life which now spans some 16 years since I became a lawyer, and from the perspective of a local prosecutor, state prosecutor and Federal prosecutor. And the views which I will express today I think have their roots in all of those areas, and I should make clear at the outset that what I say today represents my own personal views. I have not consulted with the Attorney General or anybody from the Department of Justice about any testimony to be given today, so they have not approved my statements in advance and, indeed, I don't know what the Department's position is on some of these issues, if they have formulated one.

So I hope you will accept my testimony in the spirit in which it is offered.

It seems to me the central thing wrong with the way we enforce the law in the United States today, with particular regard to these sorts of areas, the clash between privacy and law enforcement, if you will, is that for too long we have followed a sort of double-negative policy.

By that I mean we sometimes penalize honest, efficient law enforcement in the name of privacy when it is not necessary, and on the other hand, we sometimes fail to punish or discipline those in law enforcement who in the name of law enforcement break the law or abuse civil liberties.

And we think this policy is satisfactory. It seems to satisfy competing desires. Actually, it satisfies neither. It is counter-productive to efficient law enforcement. It is certainly counter-productive to Constitutional notions of liberty and privacy.

That is to say, what has usually happened in America at least in the past is where police officers or prosecutors go wrong, their brothers cover up their sins, pretend they don't exist, don't prosecute them. And, on the other hand, when we get to feeling guilty about that, we take, as a way out, the passage of restrictive legislation which impacts on all police officers, honest or dishonest, abusive or nonabusive, and in some cases actually interferes with the ability of honest police to enforce the law.

I think that is such an extraordinarily counter-productive concept that I am surprised that the professionals in the business haven't done something about that, but because politics and law enforcement are always mixed up in this country maybe it is not surprising.

It seems to me we ought to change our philosophy and adopt as our philosophy something on this order.

Consistent with our present Constitutional limits and whatever the Supreme Court of the United States may ultimately determine them to be, we ought to try to reach common agreement on zones of privacy into which nobody may intrude, even law enforcement in the name of pursuing crime. Once the boundaries of that zone of privacy are roughly agreed on, then we ought to arm our law enforcement people with all powers necessary to combat crime outside that zone with the proviso that if law enforcement officers abuse the power that we give them, either because they are incompetent or they are corrupt or they are tyrannical, that the solution to that is to get rid of those incompetent or tyrannical or corrupt law enforcers and leave the honest people with the power necessary to fight crime.

That philosophy, it seems to me, if carried out in practice, would benefit the nation and its people, would give promise of reducing crime, reducing the terrible injuries that people suffer when they are

the victims of crime, would make us a more honest and law-abiding society both from the citizen's standpoint and from the government's standpoint.

But I don't think we have had the courage of our convictions in this country yet, either on the law enforcement side or judicial side or political side or legislative side to admit that is what is really wrong here. And, as a result of that, we sometimes find ourselves getting into endless debates on this and other issues and then it seems to me it boils down to code words we all fight by. "Stop and frisk". As a law professor and prosecutor I have been in endless debates on "Stop and frisk."

When you think about it and realize it is a policeman investigating suspicious conduct in a reasonable manner, that is something that all of us as citizens would want him to do. And if a police officer intends to use the power of his office to harass or abuse citizens for whatever motive occurs to him, he will do it whether there is a stop and frisk statute, whether there is an arrest statute, whether there is a Constitution or not. It makes no difference.

You could apply the same analogy to things like "preventive detention" and the use of bail by multiple offenders—whole areas of law enforcement which spur on these debates. And I suggest that most of them usually flounder because we always end up ducking the real issue, not having the courage of our convictions to say to our law enforcement people, "Look, we want you to be straight and honest. You can't have respect for the law unless people respect law enforcers. People don't respect law enforcers who are tyrannical or corrupt or abusive or incompetent."

With that as a premise, I will turn to some specific comments about the subject of eavesdropping and wiretapping, again from the same perspective of, I guess you would say, the professional prosecutor.

We generally don't have too many problems in the Northern District of Illinois over the present statute.

I asked the FBI to gather for me the statistics on Title III's that have been implemented since I have been United States Attorney, since November of 1971, and I find they amount to 18 Title III's by the FBI in that period of time, 17 of which were gambling cases.

Though I do not have similar documentation from the DEA, my recollection of current cases is that Title III's have been useful in cocaine conspiracies, which ultimately went to indictment and trial in the Northern District of Illinois.

By far the greatest number of electronic surveillances that we employ and find useful are consen-

sual overhears rather than Title III wiretaps. Particularity is this true in the field of official corruption.

The state of Federal-state relationships in Illinois in the area of organized crime and corruption is practically non-existent, for one very simple reason: Illinois has not implemented the Federal statute with a procedure whereby wiretapping could be employed, and they have a consensual overhear statute only with the permission of the State's Attorney. Therefore, when it is necessary to intercept communications without the consent of anyone, the only people with the power to do that in Illinois are the federal authorities.

Therefore, investigations of that sort become almost exclusively Federal property and there is really no chance for us to demonstrate in Illinois, under the present Illinois Criminal Code regarding eavesdropping, the utility of joint Federal-state investigations into organized crime insofar as eavesdropping and wiretapping are concerned. So I speak from a lack of practice in that area. Perhaps other witnesses from other jurisdictions where there are implementing state statutes can be more helpful to you in that regard.

I think the power of the Federal Government to employ consensual overhears is essential to fair prosecution of cases involving official corruption, which I regard as organized crime.

Particularly is that true when the potential subject of the offense is an elected state official whose defense, feigned, or real, may well be that the moneys paid to him were campaign contributions.

The whole notion of campaign contributions in return for promises of legislative action or executive appointment or favorable policies toward public policy questions is one that is the subject of current collateral debate in this nation, and I don't intend to get into that. But there are certain areas where everybody would commonly agree that a specific agreement to trade something for cash is a bribe.

The defense of campaign contributions clouds this area for a prosecutor. And I don't know of any prosecutor who wants to prosecute someone on a doubtful or weak case. We certainly don't. We regard it as useful in making pre-indictment prosecutive judgments if we are so fortunate as to be in a position where a consensual overhear will clear the air.

We have had some recent experience with this in the Northern District of Illinois. We have returned indictments against approximately 8 members of the Illinois General Assembly. Those cases are pending for trial, so I can't be specific in my comments, but it is public knowledge that during the

course of our investigation electronic surveillance involving consensual overhears was employed. The specific devices employed were Kel sets.

And though the conspiracies at which the investigation was aimed had their inception some years before in the General Assembly, they were alive to the extent that most of the conspirators were still around, still members of the General Assembly and still talking to each other. And we found ourselves in a position where we were able to utilize consensual overhearing.

We did it for two reasons.

First, the traditional law enforcement reason, to gather any available evidence that would be helpful in proving the crime that we suspected; and, secondly, because elected legislators were involved and the defense was quite likely to be campaign contributions. If that were so, we wanted to know it before anybody was indicted. We want our prosecutive judgments to be made on all known facts, favorable to the prosecution and favorable to the defense.

I repeat it does no one any good, least of all a prosecutor, to bring cases that cannot be won or should not be won.

And in the consensual overhears involved in the legislative investigation we obtained information that persuaded us that bribery was involved, bribery indictments were returned.

We have had similar situations involving ongoing crime. The most recent one I can recall happened just a couple of weeks ago. An accusation was made that a lawyer assigned to the Federal Defender Panel was shaking down the parents of his indigent client for money—a very grievous charge, and one which, if true, is not only contrary to professional ethics but perhaps a violation of the Civil Rights Statutes of the United States, and one which threatened to stain the otherwise honorable record of the lawyers assigned to the defense of the indigent in the Northern District of Illinois. Because a potential Federal Civil Rights violation was involved, the United States Attorney's Office and the FBI employed consensual overhears to determine the truth or falsity of that allegation.

It is a sort of off-beat example but one which illustrates my central thesis that electronic surveillance and recording I think are essential to law enforcement because they come as close as is humanly and technologically possible to finding out the truth.

There are rare instances in law enforcement in my opinion where the pursuit of truth runs into higher values, whatever that may be. The essential zone of privacy is one, I know. If we did not have the ability under the Federal statute to employ con-

sensual overhears we would be severely hampered, in my opinion, in fighting organized crime, including official corruption. We would have to rely much more often on the word of accomplices, informants, people with motives to lie. And I don't think that serves either the cause of law enforcement or the cause of the defendant, whether rightly or wrongly accused.

One technical point, since it has arisen recently in Illinois. The 7th Circuit Court of Appeals has held that Federal law enforcement officers are not bound by the provisions of the Illinois Eavesdropping Act so we do not need permission of the State's Attorney in order to conduct overhears. The supremacy clause overrides the Illinois statute, although I recall one investigation I regarded as particularly sensitive, so for purposes of law enforcement comity between fellow prosecutors, I told the State's Attorney about it ahead of time and got his permission. But that was an act of comity and not a requirement of the statute.

There have been proposals made to require court orders for consensual overhears. There is now no requirement under the Federal Eavesdropping Statute to require the permission of a Federal Judge regarding overhears but—in one instance—we did regarding members of the General Assembly, but because we regarded that as so sensitive an area, we wanted the sanction of the Federal Court before we employed the device against elected representatives of the people. And we did furnish probable cause for the overhear order. It is the only time we have ever done it. And I would not do it again unless a similar situation would arise where the public policy issue was so sensitive that I wanted that additional weight on my side when public disclosure of the eavesdropping was going to be made, as it ultimately was. It was sort of a political decision rather than a legal decision, but I think it would be a sad day indeed if, either by virtue of state law or Federal law, Federal law enforcement authorities were forced to go before judges and have to show probable cause before they could set up consensual overhears.

So I think they are useful. I think the present Federal statute strikes a fair balance, so far as I can tell, at least as it applies to our operations. I think electronic surveillance and recording either by interception on probable cause or consensual overhear without probable cause gets at the truth in some very difficult areas of prosecution which, according to the temper of the American people, and I think the demands of decent government, have to be pursued.

That is about all I have to say. If the Commission has questions, I will be pleased to answer them.

MR. REMINGTON: I am sure there will be questions.

Judge Shientag.

MS. SHIENTAG: As a former Assistant United States Attorney myself, I can understand your problems and I appreciate very much your putting them on the philosophical basis that you have.

I think rather than ask questions I might commend Mr. Thompson for his excellent approach to this which, at this particular juncture of our hearings, is extremely valuable.

MR. THOMPSON: Thank you.

MS. SHIENTAG: Because tomorrow we will hear from opponents and we have already heard from a good many sources with which you are identified.

MR. THOMPSON: Thank you.

MR. REMINGTON: Mr. Blakey.

PROFESSOR BLAKEY: Mr. Thompson, I am very intrigued by your getting an Oswald-type warrant in a legislative case. Can I ask you as a former law professor what rule of Federal Criminal Procedure authorized you to get a warrant? Surely 41(e) doesn't.

MR. THOMPSON: I don't think we employed a Federal Rule of Criminal Procedure.

PROFESSOR BLAKEY: Pardon?

MR. THOMPSON: I don't recall, Professor Blakey, whether we utilized a Federal Rule of Criminal Procedure or whether we simply went to the judge and said, "Here is what we have. Will you sign an order?" I would have to see the document again. I just don't recall.

PROFESSOR BLAKEY: Did you do any research to see whether there was any authority to issue warrants, independent of the rule?

MR. THOMPSON: I doubt that.

PROFESSOR BLAKEY: There is a general catch-all rule at the end. Correct me if I am wrong, but I think it is 57(b) and it says you can proceed in any way not inconsistent with the other rules.

MR. THOMPSON: I think it was more what happened in the Hoffa cases.

PROFESSOR BLAKEY: Did you file an inventory?

MR. THOMPSON: We did in the 2.04 conference. Let me explain that in our district we have a Rule 2.04 which provides in essence a discovery process before trial. And during that conference we turned over to the defendants copies of the recordings and transcripts and everything connected.

PROFESSOR BLAKEY: After indictment?

MR. THOMPSON: Yes.

PROFESSOR BLAKEY: How long in point of time from the point at which recordings were made to indictment?

MR. THOMPSON: Oh, several months, I guess.

PROFESSOR BLAKEY: Clearly longer than the ten days provided for inventory in 41?

MR. THOMPSON: Yes.

PROFESSOR BLAKEY: Do you know whether there is legislation now pending in the Illinois General Assembly to put further restrictions on one-party consent for surveillance?

MR. THOMPSON: I have heard there are but I am not familiar with the specifics of the bill.

PROFESSOR BLAKEY: Do you think there is any relation between that legislation and your prosecution?

MR. THOMPSON: Possibly.

PROFESSOR BLAKEY: Let me ask you to comment on this. I have had this put to me by other people who have worked corruption cases. They say one of the most difficult dilemmas they face is when they get an allegation that is, say, fair on its face, perhaps, but not credible, of corruption, and an investigation is made, and you don't have a hard case; you have a soft case. The great dilemma you face is that if you don't prosecute it you are later accused of corruption and if you do prosecute it and you lose it, you are accused of political witch hunting.

MR. THOMPSON: Yes.

PROFESSOR BLAKEY: And if you win it, you always have a bad taste in your mouth that you may have convicted an innocent man.

MR. THOMPSON: Well, I have been through the mill with all of those accusations and I count that statement as correct. I have sort of inured myself to it now because we take the position in our office that you can't be a decent, fair, effective prosecutor if you are afraid. You must never be afraid to do what you think is right. I think that probably sums up the motto of our office that at all junctures prosecutors take risks and take chances. During my administration—in fact, two weeks after it began—I signed my name to an indictment of a sitting Federal Judge. It is the first time in the history of the country a sitting Federal Judge was indicted and convicted.

PROFESSOR BLAKEY: How about Judge Mawton?

MR. THOMPSON: I think all the others retired before they were convicted. And if I had lot that case I might not be here today. That I know.

And yet the defenders of that defendant, and he, himself, still pursue me. It has come full circle now and the prosecutor is on trial.

That is part of the risks of the game.

I find it to be, as you say—sitting in my office, as you might well imagine, during the last four years I have heard allegations about corruption on the part of just about everybody. A lot of them are obvi-

ously crank allegations that can be dismissed off-hand. Some of them warrant preliminary inquiry. Some of them warrant more intensive grand jury investigation. Some of them warrant agency investigation. Some of them may even warrant electronic surveillance.

They range in degree from crank to dead serious.

But when you are in government, you eventually come to know that in a great metropolitan area like Chicago not a day goes by that you don't hear some story about somebody. And ultimately the responsibility and the weight of those stories come back on the prosecutor's shoulders.

I have often said lately, as I have grown more reflective after nearing the end of my first term as a United States Attorney, that the public will probably see and understand only about one-tenth of our work. Nine-tenths is forever buried—cases that aren't made, allegations that go nowhere, instances in which the grand jury acquits people, in which Federal investigative agencies acquit people who are not subsequently charged and whose reputations are not tarnished and whose lives are not destroyed. And those acquittals come about sometimes as a result of using the very same investigative techniques and devices that sometimes convict people.

And it is very hard for people who are not in prosecution or investigation or associated with those disciplines to understand that. That is absolutely true.

PROFESSOR BLAKEY: Your comment raises a broader question. We have had testimony before the Commission on a number of occasions that the use of these kinds of sophisticated investigative techniques requires sophisticated professional legal advice, either in the context of a Strike Force or in the United States Attorney's office. I wonder if you would comment on that.

Can you do this kind of investigation without lawyer participation?

MR. THOMPSON: Well, I come out of the state system where the investigators work for the prosecutor. So my entrance into the Federal system where the investigators do not work for the prosecutor, work for themselves, was somewhat shocking. I have become somewhat inured to the fact that the FBI and DEA and IRS don't work for me. They work with me quite well, but I can't give them orders. But for the past five years, as we have intensively gone into the organized crime and official corruption areas, we have sort of changed the system somewhat, so now there is much earlier participation by lawyers in the investigatory process than was probably true before we came. And it is somewhat like the state system that I was used to, although not entirely.

We make much more frequent use of the investigative grand jury than has ever been made before in the district. And within the bounds of propriety, so far as the regulations of the investigative agencies are concerned, sometimes my men will be in right at the beginning. And I am all for that on a broad basis. I think investigators and lawyers ought to be together at the beginning of any investigation as a general policy. And since I think it is especially true in the kinds of cases in which we specialize, national crimes, official crimes, organized corruption, I think when you deal in this sensitive and sometimes technical area of electronic surveillance, lawyers ought to be in there right from the beginning—especially post-Watergate. Watergate has scared the hell out of a lot of investigative agencies, especially as far as things like electronic surveillance are concerned. They are very sensitive to it.

Because so many Federal agencies have been accused of doing things they didn't that they may have been importuned to do but didn't do—sometimes we find it difficult to utilize practices like electronic surveillance. We have to go higher up in the agency to get permission. It takes longer to get permission and to get the equipment and we run into bureaucratic delay, but we get it.

But Watergate and its accusations have burned everybody a little bit—and I think unfortunately.

PROFESSOR BLAKEY: Is there a Strike Force in the Northern District of Illinois?

MR. THOMPSON: There is.

PROFESSOR BLAKEY: What is the relationship between it and your office?

MR. THOMPSON: Well, I would characterize it as excellent. When I came there in 1970 the Strike Force consisted of maybe two or three lawyers. And their lack of resources severely hampered them in their ability to be both innovative in terms of investigative devices and prosecutorial techniques and to grind out a steady flow of organized crime prosecutions, as is their day-to-day mandate.

And I am one of those United States Attorneys who not only cooperated with Strike Forces but went to the Department of Justice to ask for more resources for them. Because for a long period of time all significant Strike Forces cases had to be carried out as joint United States Attorney-Strike Force projects. They still are, even though their resources are now triple what they were when I came.

I went down and pounded on Henry Petersen's desk and said, "Give them more men," and he did.

They are like a division of our office, although they are not responsible to me. We communicate

back and forth very well. It is a matter of personality, I think. We are not jealous of each other.

PROFESSOR BLAKEY: Do you think that is unique?

MR. THOMPSON: It was at one time unique in the Department of Justice in my experience. It is becoming somewhat more common, although, as a matter of public knowledge, there is still considerable debate within the Department as to whether or not Strike Forces ought to exist, or at least whether their original rationale ought to be re-examined.

PROFESSOR BLAKEY: Is hiring in your office without regard to race, color, and creed, or political affiliation?

MR. THOMPSON: Yes, sir. The very first priority of our office was to take it out of politics if it was in there when we got there. Although I must say that enough credit has not been given to our immediate predecessor, Mr. Foran, who was United States Attorney for about a year and a half before I came in there.

He had begun the process of non-political hiring. We wiped it out completely and I have probably hired 60 lawyers in the last five and half years, first as First Assistant and then as United States Attorney and not one has been hired as a result of the political patronage system. There may be one or two in the office who have had some political experience which we count as a plus if it gave them a greater advantage in working with people, and which we counted as a minus if they thought it entitled them to a job. And everyone who came into my office with a resume that included some political experience was questioned closely on that point and if there was any question that it entitled them to a job, the application went into the wastebasket and they weren't hired.

As a result, out of a staff of 66 lawyers we may have 10 or 12 people who have spent time in politics and they worked for such persons as Senator McGovern, President Nixon, Senator Stevenson, Governor Walker, Governor Ogilvie, Senator Percy—all parties, all philosophies.

PROFESSOR BLAKEY: What is the experience level?

MR. THOMPSON: It varies. We started by hiring young people right out of law school. We had a fair number of lawyers held over from previous administrations which we counted as a very valuable experience for us.

It depends somewhat on economic times. When times are tough on the outside job market, we will find more applications from Harvard, Yale, Chicago, and Michigan. As the reputation of our office spread we also found those same sorts of applications coming in.

Within the last year or year and a half we have hired a number of people who have invested three or four years in a top-flight law firm but found they weren't getting trial experience and took considerable cuts in pay to leave the firm and come with us.

We have no preconceived notions about hiring, geographical preference, grade point average, race, color, or creed. We have never "recruited" except for two areas—blacks and Spanish-speaking. Because of the shortness of supply there, we have recruited. We went from no women lawyers in 1970 to nine, including the first two women chiefs in that office. We will have this fall three black women lawyers, which I think is more than any other United States Attorney's Office in the country.

We look for bright young people who believe in the same things we do: integrity, willingness to work hard, and the notion that public service is the best job there is and they are damn lucky to get it and they probably won't have it for very long, and it may be the most exciting years of their lives. If we think they believe in that, we hire them.

With those kinds of standards, politics just are not relevant.

We have also found that with a non-political method of hiring, we more easily assure ourselves, and I think in turn assure the public, that when we work cases involving official corruption, which cases necessarily involve politicians, we are a lot further down the road toward insuring there are not partisan motives in the prosecutions we bring. If the loyalty of an assistant runs to me and to the people of the district rather than to a Senator or a Ward boss or a party or a philosophy, we are protected and the citizens of the district are protected against partisan prosecutions. And they are protected even if I were to go wrong. There is a self-protective device there that if I suddenly harbored political ambitions and used the powers of my office for political reasons, the 76 men and women there would be so offended by that that they would be out.

PROFESSOR BLAKEY: How typical is your office of United States Attorneys throughout the nation with the exception, say, of the Southern District of New York and maybe the Northern District of California?

MR. THOMPSON: Well, I think it is typical of some others. I think it is typical of the District of New Jersey. I think it is typical of Detroit—Southern and Northern California.

You see a sort of revolution took place in the United States Attorneys Office during the past five or six years. And ironically a national administration and a national Department of Justice which

later had its own share of troubles so far as enforcement of the law in Watergate was concerned was probably the Administration which did more to professionalize and upgrade United States Attorney's Offices than any Administration in the prior history of the country.

And much of that credit has to be given to a man who, himself, was ultimately caught in the coils of criminal law, Dick Kleindienst, who insisted that United States Attorney's Offices become more professional, be given the resources to do the job, be allowed to proceed without political interference from Washington. And it is sort of an ironic thing but you can track it in this country, of young prosecutors being hired non-politically, of United States Attorneys coming up through the ranks. The District of New Jersey and the Northern District of Illinois are examples of that.

Let me show you my district as an example.

My First Assistant is a young lawyer by the name of Samuel Skinner, who was first hired eight years ago under a Democratic administration and he was assigned as an Assistant United States Attorney in the Claims Section of the Civil Division. He has risen through the ranks to become the First Assistant United States Attorney. If I were to walk out of this building today and get run over by a truck I assume the court would appoint him as United States Attorney. That would be quite an achievement for that young man.

The Deputy United States Attorney is a man who has served 20 years in the United States Attorney's Office and twice been Chief of the Civil Division and twice Chief of the Criminal Division there, a distinction shared by nobody else in the country, to my knowledge.

The Chief of my Criminal Division was hired by a former Democratic administration and has come through the ranks to his supervisor's position.

They have all come through the ranks.

My former First Assistant three months ago was appointed as a Federal District Judge, the youngest in the nation. He is the man who, eight years ago, couldn't become an Assistant United States Attorney because he didn't know who his ward leader was in Chicago. And he has gone to the Federal bench.

These sorts of success stories I think are the product of the philosophy of law enforcement that we employ, and it is a product of the philosophy of law enforcement that we were allowed to employ under an administration of the Department of Justice which in this city and in other contexts had tragic problems.

PROFESSOR BLAKEY: Thank you, Mr. Thompson.

MS. SHIENTAG: May I ask a question?

MR. REMINGTON: Judge.

MS. SHIENTAG: You said if you were to be struck by a truck your First Assistant could take your place adequately.

There is a common rumor that the next First Assistant to Mr. Levy would be a United States Attorney. Now, if you were struck by lightning would there be the same likelihood a First Assistant would be likely to take your place?

MR. THOMPSON: I respectfully decline to answer that. I have the greatest of respect for Dean Lavy who I think will prove to be one of the finest Attorneys General and there serves under him a Deputy Attorney Judge for whom I feel an equally high regard, Judge Harold Tyler. So I think the Department of Justice is in safe hands.

MS. SHIENTAG: But you have heard the rumor that the next Assistant would be a United States Attorney from one of the districts?

MR. THOMPSON: I have not heard that rumor.

MR. REMINGTON: Chief Andersen.

CHIEF ANDERSEN: Mr. Thompson, in view of what you are saying, do you think it is time under Title III that the wiretap permission should be removed from Washington?

MR. THOMPSON: I think as a practical matter it probably wouldn't make too much difference. In my experience as United States Attorney I don't think we have ever had a Title III request turned down.

Now, if we have, maybe one or something like that.

On the other hand, all United States Attorney's offices don't operate at the same level of experience or sophistication, and that is not to denigrate my fellow United States Attorneys: it is simply a reflection of the fact that there are 76-man United States Attorneys offices; 2-man United States Attorneys offices; 120-man United States Attorneys offices; and talents may ebb and flow at times in those departments.

I assume the bureaucracy of the Department offers a continuum and stability and precedent and prior experience that may be useful in determining whether Title III permission should be granted, although, on the other hand, it is probably likely that most Title III applications come from those offices which possess as much expertise in the field as they do in Washington, or even more.

So I don't think it is really a burning question. I don't think it will have much practical impact one way or another.

CHIEF ANDERSEN: You don't think it is a burning question in Title III?

MR. THOMPSON: No.

CHIEF ANDERSEN: Do you follow the *Jones* decision or do you give information to state and local authorities from wiretaps?

MR. THOMPSON: No, I don't think we turn over.

CHIEF ANDERSEN: So you are literally following the California *Jones* decision?

MR. THOMPSON: Yes.

CHIEF ANDERSEN: It brings up an interesting question because Illinois is the only state I am aware of that has both a consensual recording law and a wiretap law. Would you take the same attitude toward information obtained through Federal consensual recording which you wanted to turn over to state authorities in Illinois where consensual recording is permitted by law?

MR. THOMPSON: Oh, if we gathered information by consensual overhear, I think we would turn that over to the State's Attorney's Office if the occasion arose, since the State's Attorney, himself, would have done the very same thing had he initiated the investigation. He certainly would have given himself permission to do it.

CHIEF ANDERSEN: If the question came up it would be the equivalent to the *Jones* decision on wiretapping?

MR. THOMPSON: I don't think the question has come up in our office, frankly.

CHIEF ANDERSEN: It just hasn't arisen?

MR. THOMPSON: No, not that I am aware of.

CHIEF ANDERSEN: Thank you. I have no further questions.

MR. REMINGTON: This morning I asked a question that I think is basic and relates to some extent to your earlier statement, that you think there is an area of privacy that ought to be recognized and outside of that law enforcement ought to be given effective methods of achieving its objective.

We know the area of electronic surveillance is not the only area of concern. There is, for example, the area of arrest or the area of search for physical evidence.

I think it is a valid generalization that we have not seen a great deal of concern about the arrest power, although there is pending in the House of Representatives a change in Rule 4, but that has not given rise to a great deal of public concern.

With regard to Rule 41, there have been some changes made. I would daresay those changes have gone largely unnoticed in terms of public interest.

And yet at the same time in the area where law enforcement is asking for authority, with judicial approval, to listen, we see a great deal of concern, both in the creation of this Commission and several Congressional committees looking into various aspects of this.

In your judgment, is this because there is something different about listening to someone than arresting or searching him? Is it that this area is more important than those areas? Is it because there is a greater threat to individuals here than in the area of arrest?

MR. THOMPSON: I think, Mr. Chairman, it probably arises from a variety of factors.

First, we have been arrested for hundreds of years and we are sort of used to it, I guess—and searched as well. Arrests of persons in order to have them answer criminal charges is a law enforcement practice with centuries behind it and it doesn't stir the blood as newer tactics may.

We have only been overhearing or recording for a few decades.

Secondly, I suppose that arrest and search is a very specific practice, whereas overhearing has the potentiality for being an indiscriminate practice. You go out and arrest one man for one crime and search the person and that is a different sort of thing than putting a bug on one phone and risking hearing 30 persons and a hundred conversations in the potentiality. That doesn't frighten me, but I daresay it frightens some people.

PROFESSOR BLAKEY: Do you see "class" connections to it; it is not "us" who are arrested? If I were arrested, I would call my lawyer.

MR. THOMPSON: You would be allowed to surrender but in our office, Professor Blakey, almost everybody is allowed to surrender except dangerous people. But I don't know if our experience is typical.

PROFESSOR BLAKEY: Let's take it over the run of law enforcement as a whole. If you are going to be arrested, you are probably black, a teen-ager, and poor, and if you are going to be wiretapped, you are probably white, upper-class and a professional?

I am not trying to put words in your mouth but isn't there a kind of "us" and "them"?

MR. THOMPSON: There is something to that, but there always has been in law enforcement. There is something to that.

The same thing is true of immunity. Nobody in this country started getting concerned about immunity until people went to jail who hadn't gone to jail before. Now there is a great raging debate on immunity.

So that may lay in back of it.

Anything which threatens the establishment or the powerful is bound to bring out the anxieties of the establishment or the powerful even though they don't feel themselves personally involved.

Yes, sir.

MR. REMINGTON: I suppose you might say that listening to other people threatens the Democratic process, whereas arresting and searching does not. Would that be a position that is tenable?

MR. THOMPSON: I don't think that is a tenable position simply because professionals know that the mechanics won't admit of it. There aren't enough people to man the bugs to eavesdrop on all the people in the United States who imagine they are being eavesdropped upon. That is just an unavoidable fact.

We don't do it. It is expensive; it is time-consuming. It is a lot of hassle to engage in electronic surveillance, even consensual overhears. We really only use it when we think it is likely to be productive of the truth in an unclear area.

And I daresay most prosecutors and police feel that way.

I also daresay there is probably a fair bit of unlawful eavesdropping going on in the United States, both in the law enforcement area and in the non-law enforcement area. We follow the mandate of the Department of Justice to vigorously prosecute that. We had two and I think another one this week on unlawful wiretapping.

We have one in the grand jury of unlawful wiretapping by the Illinois Bureau of Investigation. It is a hard problem to wrestle with.

If people are out to unlawfully wiretap or eavesdrop, be they private citizen or policeman, and whether they are doing it from a corrupt motive or from a mistaken law-enforcement motive, it doesn't make any difference what the law is or isn't, whether the prosecutor is there, whether there is a likelihood they will be found out and prosecuted. They will do it, just as the policeman who is bent on harassing the ghetto black will do it whether or not there is a "Stop and Frisk" statute or an arrest statute.

You can't strike at unlawful, evil, willfully motivated conduct by restricting the powers of honest law enforcement officers. And yet that is what we have really been doing without admitting it to ourselves in this country for a long time.

MR. REMINGTON: I think it has been said by someone that the appropriate way to proceed is to give law enforcement half of the authority they need on the theory they will use twice what they get and it will turn out just about right.

I take it you disagree with that?

MR. THOMPSON: I disagree very violently with that philosophy.

MR. REMINGTON: Mr. Thompson, one last question.

This Commission is asked basically to address the question of whether authority to conduct electronic

surveillance is needed and whether Title III as presently administered is effective and adequately protective of civil liberties.

How would you answer that?

MR. THOMPSON: If I were to answer both of those questions in a general fashion I would say the answer to both of them is yes.

I think the authority is needed and I don't think the experience we have had so far from Title III has demonstrated that civil liberties are abused by court-ordered eavesdropping.

MR. REMINGTON: Okay.

Do you think there is anything else this Commission ought to know this afternoon?

MR. THOMPSON: Undoubtedly there is, but you have exhausted me, I am sure, and I have probably exhausted you.

MR. REMINGTON: No, thank you very much. You have been very helpful and we appreciate it very much.

We will take a five-minute recess.

[Whereupon, a short recess was taken.]

MR. REMINGTON: May we reconvene for the purpose of hearing Mr. Phillips.

Mr. Phillips, we are pleased that you are here, and sorry it has taken us as long as it has to get to you. I hope keeping you this late hasn't inconvenienced you too much.

MR. PHILLIPS: It is quite all right. I appreciate the invitation.

MR. REMINGTON: Mr. Phillips is Special Prosecutor for the City of Philadelphia which position he has held for a year. Prior to that time he was Assistant District Attorney for New York County and has had experience in a setting where electronic surveillance is authorized, and most recently in a setting where there are the most stringent prohibitions against the use of electronic surveillance. He is in a particularly good position to give us a statement about both of these alternatives.

Before that we will ask you to be sworn.

[Whereupon, Walter M. Phillips, Jr. was duly sworn by the Chairman protem]

TESTIMONY OF WALTER M. PHILLIPS, JR., DEPUTY ATTORNEY GENERAL, OFFICE OF THE SPECIAL PROSECUTOR, COMMONWEALTH OF PENNSYLVANIA

MR. REMINGTON: Mr. Phillips, we all have a copy of your written statement and so, if you will agree, without objection it will be made part of the record.

MR. PHILLIPS: Certainly.

[The prepared statement of Mr. Walter Phillips follows.]

STATEMENT OF
WALTER M. PHILLIPS, JR.
DEPUTY ATTORNEY GENERAL
OFFICE OF THE SPECIAL PROSECUTOR
COMMONWEALTH OF PENNSYLVANIA

I. Introduction

I am the state Special Prosecutor for the City of Philadelphia. The Office of the Special Prosecutor was established by the Attorney General of Pennsylvania in April 1974 to investigate and prosecute corrupt police and public officials in Philadelphia. Corruption investigations can be divided between overt investigations of past acts of corruption and covert or undercover investigations of present corruption. The former is generally carried out with a grand jury whose subpoena power can be used initially to obtain documents and later to compel testimony. The latter requires the use of informants and others acting in an undercover capacity, and it is in these investigations that electronic surveillance plays a vital and sometimes indispensable role.

Pennsylvania currently has the strictest anti-electronic surveillance law in the country. In 1957, a law was passed by the Pennsylvania legislature, entitled right to privacy law, that prohibited any type of telephonic interception. Thus, even where one party to a telephone conversation consented to having the call recorded, it could not be done without violating the law unless the other party also consented. There was no provision even for a court order making it legal.

In November 1974, the legislature approved a bill known as an anti-eavesdropping bill that amended the right to privacy law. This bill made illegal any recording of a conversation, whether over the telephone or in person, unless all parties to the conversation consented to its being recorded. There is just one exception to this prohibition, and that is where a law enforcement officer believes that his personal safety is in jeopardy and has obtained a court order through an application being made by the Attorney General or the District Attorney; but even then the tape recording is not admissible in a subsequent court or administrative proceeding. Despite protestations by myself, other prosecutors and even several well known civil libertarians, Governor Shapp signed this bill into law. As a result, it is now forbidden for a law enforcement agency to obtain evidence of a crime by placing a tape recorder on one of its agents or a cooperating individual to record criminal conversations of a corrupt police officer, narcotics trafficker or other person violating the law.

II. One Party Consensual Monitoring

The ability to record conversations of public officials as they engage in corrupt transactions is by far the most important investigative technique to any agency investigating ongoing police and official corruption. Tape recordings provide valuable corroboration to prosecution witnesses who invariably are individuals of a highly unsavory character. Police corruption involves receiving protection money from gamblers, narcotics traffickers, prostitutes, etc. Juries naturally require substantial independent corroboration to the testimony of these individuals before they will convict a police officer, and recordings of conversations between the prosecution witnesses and the defendant police officer provide better than any other type of evidence this corroboration. Also, tape recordings in a corruption case can offset the defendant's strongest defense, that is, his impeccable reputation, background and appearance in the courtroom. Bringing to the jury's attention the defendant's other personality through tape recordings of him receiving a bribe payoff can become critical to the prosecution's case.

There have been some recent examples of the reaction of juries and judges to tape recordings in criminal cases. The day after the Watergate coverup case was concluded, the jury foreman was quoted as saying that while Dean, Kalmbach and Magruder were credible witnesses, by far the strongest evidence introduced by the Government were the White House tapes, because they were uncontested. In fact, he even remarked that it was "too bad they can't have tapes at all trials. It would help the jury a lot." Recently, the Second Circuit Court of Appeals was confronted with the question of whether to overturn the conviction of a criminal defense attorney who had been convicted of paying off an admittedly corrupt police officer to obtain certain information. The issue was whether admissions made after trial by the corrupt police officer, who was the principal Government witness, of wrongdoing on his part that he had lied about on the witness stand should warrant a new trial. The Court in affirming the conviction found that the tape recordings of conversations between the attorney and the corrupt police officer were the "underpinning" of the Government's case, not the testimony of the witness as contended by the attorney.

One party consensual monitoring is particularly vital to any meaningful investigation of gambling related police corruption. In order to avoid harassment through arrests and raids, major gambling operations in big cities such as Philadelphia and New York have been found to pay off entire units of plainclothesmen. The *modus operandi* is that generally a "bagman" who is one of the officers in the unit will collect the money directly from the gambler and distribute it among the rest of the unit. Assume for the moment that the corrupt bagman, for whatever reason, decides to cooperate with a prosecutor to gather evidence of corruption against those for whom he has been collecting payoffs. Unless the bagman can be equipped with a tape recorder to record the transactions with the other police officers, the only strong corroborating evidence that can be obtained to support the bagman's testimony later in court is the use of marked money seized immediately upon receipt of it by one of the officers. However, such a seizure and arrest will obviously surface the cooperating bagman, thereby terminating the investigation and eliminating the possibility of any further arrests of other corrupt policemen in the unit. If, on the other hand, the bagman can continue his corrupt dealings with the police officers in the unit, tape recording conversations and transactions as they occur, the likelihood of making numerous cases that will stand up in court is very good. Certainly the overall impact on the corruption problem will be greater if it can be shown that there is not just one corrupt police officer but an entire unit on the pad; that is, that the barrel is rotten, not just one apple.

Finally, a tape recording is the most effective and sometimes only way to obtain a corrupt police officer's cooperation in making cases on other corrupt police officers. This is done by confronting a police officer with a tape of his engaging in a corrupt transaction so that he sees first hand how strong a case exists against him. Corrupt police officers will only cooperate against their fellow officers when they will go to jail. This has been done both in Philadelphia and New York resulting in the prosecution of a number of substantial police corruption cases.

Since one party consensual monitoring is now illegal in Pennsylvania and since police corruption cases that have the most impact and significance are those where police corruption is detected while ongoing, it is just about impossible to conduct meaningful investigations of police corruption in Pennsylvania. Federal law permits this type of electronic surveillance without a court order, and this is as it should be. The argument is often made, and the law in some states is, that a court order must be obtained before a law enforcement agency can wire up an individual to record a criminal conversation. I do not share this view. The purpose of a court order, as in the case of search warrants, is to place a judicial imprimatur upon an uninvited invasion of privacy, and therefore insure against unreasonable inva-

sions in violation of the Fourth Amendment. Where, however, the party who consents to the conversation being recorded is reporting his conversations to a law enforcement agency and will be a witness later against the other party to the conversation, the taping of the conversations is really no invasion of privacy at all. Thus, when a corrupt police officer, for example, engages in a conversation or transaction with a gambler to solicit a payoff from that gambler, the police officer's privacy and confidence in the gambler is violated when the gambler reports the conversation to a law enforcement agency and then testifies about it. Tape recording the conversation to corroborate the gambler's testimony is simply cumulative of the primary violation of that privacy.

Thus, since the Fourth Amendment and cases decided under it do not require a court order in a one party consensual monitoring situation, and since it is difficult to conceive how this investigative tool could be abused, I would be opposed to any legislation requiring a court order before law enforcement can use body wires. New Jersey just recently revised their electronic surveillance statute to require the authorization of either the Attorney General or a district attorney before a tape recording of this type can be used. Such an authorization gives an official seal of approval to its use and limits its use for law enforcement purposes, and since the only real legitimate use of one party consensual monitoring is for law enforcement purposes, I would not be opposed to such legislation.

III. Wiretapping and Non-Consensual Monitoring

Wiretapping is a far greater intrusion of privacy than one party consensual monitoring because with wiretapping neither party to the conversation that is being intercepted has consented to have it recorded. Wiretapping also often involves the interception of whole or parts of entirely innocent conversations. On the other hand, wiretapping can often be the only way to make a prosecutable case against the higher-ups of a major narcotics or gambling operation, or provide the necessary corroboration against the public official who arranges a corrupt transaction over the telephone. For these reasons, I believe that wiretapping should be available to law enforcement but only under the strictest court supervision.

Wiretapping is especially vital to law enforcement in the area of gambling if any of the top members of the gambling operation are to be prosecuted. A major gambling operation, whether it is a numbers bank or a sports betting operation, uses the telephone extensively, in fact depends on the telephone to conduct its daily business. Contact between the major figures of the operation and their writers, the placing of bets by established and well-paying customers, as well as the "laying off" of bets, are all done exclusively by telephone. Every major federal and state gambling case prosecuted in New York while I was in the United States Attorney's Office there was done through the use of wiretapping.

Because wiretapping is illegal in Pennsylvania, major gambling cases are rarely if ever prosecuted by state authorities. Almost all cases prosecuted in the state courts in Philadelphia are numbers writers who are arrested pursuant to a search warrant and prosecuted based on the number of numbers slips found on them. In 1972, 91.6% of all gambling arrests in Philadelphia resulted in acquittals or dismissals, and only .4% resulted in jail sentences. These statistics reflect both the public attitude toward gambling as a victimless crime, and the lack of resources on the part of law enforcement to prosecute major gamblers. Without the ability to wiretap, the prosecution of gambling cases becomes a vicious cycle. Police officers under pressure to make arrests, regardless of their quality, resort to unconstitutional means such as perjured search warrants and bring into the court only the lowest members of the gambling operation. Judges quite naturally either throw out the search warrant or simply find the evidence insufficient to convict. Tremendous resources are devoted to the enforcement of gambling laws with little or no

return realized. I have recently testified before the Commission on Review of the National Policy Toward Gambling that unless wiretapping is made available to state law enforcement agencies in Pennsylvania, the Legislature ought to consider some type of legalized numbers betting.

Wiretapping is the only way to infiltrate and get evidence on the top members of organized crime. In narcotics, an undercover officer will only be able to deal with the street seller. In gambling, the major figures insulate themselves by having contact exclusively with their most trusted lieutenants. Yet in order to oversee the operation, whether it's narcotics or gambling, the organized crime figure must rely to a certain extent on the telephone. Narcotics transactions are many times arranged, though not consummated, over the telephone, and while coded language is employed, experienced investigators do not have much trouble interpreting the code. When conversations of this type are intercepted, the prosecution possesses first hand evidence of the conspiracy as it is occurring. While Chief of the Narcotics Unit for the United States Attorney's Office for the Southern District of New York, I directed the prosecution of several major narcotics cases where this type of evidence played a major role in obtaining convictions.

In addition to obtaining hard evidence of the conspiracy itself, wiretapping is useful in providing corroborative evidence. In narcotics cases, arrangements for meetings which can then be surveilled are discussed on the telephone. It is not unusual for one of the participants to later be cooperating and explaining to a jury what was transacted at the meeting. The apparently innocent telephone conversation setting up the meeting then takes on vital significance in corroborating the accomplice's testimony. Neither the wiretap evidence nor the accomplice's testimony standing alone would have been sufficient for a conviction, but together they provide overwhelming evidence.

In Philadelphia, there have been situations where we have had probable cause to engage in non-consensual monitoring but have been unable to do anything about it because of the Pennsylvania law. For example, several times we have received information that payoffs to police were being made in a particular bar by a major gambler. Surveillance by our agents at the bar corroborated that police officers came there and met with the gambler in a back room for a few minutes and then left. Placing a bug in that room to record the conversations would obviously have been very fruitful. In fact, confronting the gambler with a tape of his making payoffs could very likely have resulted in his being willing to cooperate against all the police officers he has been paying off.

The inability to wiretap major gamblers or public officials against whom we have obtained sufficient probable cause to believe are using the telephones to transact their corrupt business has greatly impeded our investigations. One of our investigations has led to the indictment of an individual for attempting to extort \$100,000.00 in connection with a city contract. During the investigation, we developed probable cause to believe that this individual was using the telephone to contact an accomplice in the scheme, a former city official who himself was heavily involved in other corrupt transactions involving city contracts. Had we been able to install a tap on this second individual's phone, the likelihood would have been great that we could have uncovered other corrupt situations and officials in addition to making a strong case on this person with respect to the \$100,000.00 extortion scheme. Instead, because of the law, all we now have is a case on the one individual who dealt with the victim of the extortion who was cooperating with us. Typically, the second individual had insulated himself from contact with the victim, and in turn was insulating the public officials above him in the scheme. This case shows the importance of wiretapping in providing a law enforcement agency with leads to other corrupt situations which would otherwise be unknown to it.

While I oppose judicial supervision of one party consensual monitoring, I vigorously support close judicial scrutiny of non-consensual interception. Thus I would advocate legislation similar to the present federal law requiring that a detailed written application approved by the top prosecutor of the state, the Attorney General, be submitted to a court before a wiretap or bug is allowed. For state legislation, I would urge several changes from the federal law. For one, minimization ought to be fully spelled out in the statute. Law enforcement agents should know exactly the extent to which they may intercept non-pertinent calls. The courts should not have to engage in extensive hearings to determine whether minimization has occurred.

Also, and more importantly, I would advocate that rather than permitting any judge to approve a wiretap, a panel of judges should be selected to approve all non-consensual applications. These judges should be selected from the appellate ranks and should have statewide jurisdiction to issue wiretap orders. Approval of a wiretap application should be given only after careful scrutiny—the court should not act as a rubber stamp as is the case with search warrants. The approving judge should maintain close supervision of the wiretap after it has been installed and should be provided with detailed reports from the agents monitoring the tap.

Those opposed to legalized wiretapping make the argument that legalizing wiretapping will also increase instances of illegal wiretapping because it will make wiretapping equipment much more available. It is difficult to respond to a speculative argument such as this, and there are obviously no statistics to support or disprove it. I would point out that while court approved wiretapping is legal in New York, I am not aware of a great concern there about abuses of the privilege. On the other hand, in 1972 in Pennsylvania, members of the state police illegally attempted to intercept conversations of other members of the state police engaged in a police corruption investigation by illegally bugging a motel room. Several persons were arrested but the case was thrown out at the preliminary hearing by a local magistrate. It seems to me that a solution to this potential problem would be to impose severe penalties for the illegal interception of telephonic or oral communications, and require that any violations be prosecuted by the Attorney General's office and before one of the judges on the panel designated to approve wiretaps. Such a law, I believe, would act as a deterrent to those considering engaging in illegal wiretapping.

The recent concern over illegal electronic surveillance is the result of Watergate and numerous law enforcement abuses that as a result of Watergate have come to light. I too am disturbed about the extent of these abuses, but with organized crime still having tremendous control over a large segment of criminal activity in this country, I would hope that very careful consideration be given before any further restrictions be imposed on law enforcement in the use of one of its most effective investigative techniques. I would think that strict court supervision and the appointment of responsible public officials will prevent further abuses from occurring.

MR. REMINGTON: Do you have an initial statement of some kind you want to make at this time?

MR. PHILLIPS: I thought I would summarize the statement I had provided the Commission.

You now know what the law in Pennsylvania is with respect to electronic surveillance, that is, that all forms of wiretapping are outlawed, even court-approved. And recently there has been a bill that has amended the Right to Privacy Law, outlawing automatic one-party consensual monitoring with

some narrow exceptions which do not help law enforcement at all.

I became a very outspoken critic of the bill which was pending before the Governor after being passed by the Legislature last fall and urged the Governor's veto. However, he did sign it into law and it now is the law. I think it is very unfortunate because in any type of criminal activity that involves organized crime and corruption, particularly one-party consensual monitoring, is indispensable to any meaningful investigation. And with respect to organized crime activity in the area of gambling and high-level narcotics activity, wiretapping is very important.

I oversaw a number of prosecutions in New York while Chief of the Narcotics Unit for the Southern District of New York where wiretapping played a vital role in the obtaining of convictions there of high-level individuals who you would never be able to get to with undercover agents.

With respect to one-party consensual monitoring, that is essential, particularly in corruption investigations and particularly in police corruption investigations. Police corruption involves situations where police officers have shaken down individuals of rather unsavory character. This characteristic means they are very susceptible to being impeached on cross examination in a court of law.

As a result, you have to have corroboration if you are going to obtain a conviction. And without being able to engage in tape recording a conversation between the witness and the police officer, it is virtually impossible to make a stand that is going to stand up to the unanimous satisfaction of a jury.

Without being able to wiretap, I think that there are a tremendous amount of resources in Pennsylvania that are being devoted to trying to enforce what is an unenforceable law in the area of gambling. The statistics that the Pennsylvania Crime Commission compiled for the year 1972, I think are startling, but reflect what the situation is in Pennsylvania, that is, that 91.6 percent of all gambling arrests resulted in either acquittals or dismissals and only .4 percent resulted in prison sentences for the defendants. What has happened is that without being able to wiretap, local law enforcement agencies are not able to go after the top men of the gambling operation. If they are not arresting those people and bringing them into court, the courts are not giving prison sentences. They are either throwing out the case by throwing out the search warrant or finding insufficient evidence or, if they do convict, the individual is such a low member of the operation, usually a numbers writer, that he gets a fine or probation of some type.

It is a vicious cycle. Both the resources of the police department and the resources of the judiciary are not realizing any return for their efforts.

What I would advocate is what is presently the federal law. That is, that wiretapping be legal, but only under the strictest court supervision and an order could be issued upon an application approved by the Attorney General of the State of Pennsylvania.

I would further advocate with respect to one-party consensual monitoring—again, I think the Federal law is adequate in this sense and is good and balanced in the interest of society and interest of individuals, that law enforcement be permitted to engage in one-party consensual monitoring without having to obtain a court order.

New Jersey has recently slightly revised its electronic surveillance law to require that the Attorney General or the District Attorney approve any one-party consensual monitoring on the part of law enforcement and I think this is a good idea. I know this is done federally. Although the law does not require it, the Department of Justice requires there be approval before any type of one-party consensual monitoring is engaged in. I do not think a court order ought to be required because I do not think you are talking about the same invasion of privacy that you are with respect to wiretapping.

Essentially those are my views on what this Commission is looking into and I would be prepared to answer any questions.

MR. REMINGTON: Mr. Phillips, I think Mr. Stein will question you.

MR. STEIN: Just to develop the background, Mr. Phillips, you have held your present office since April 1974; is that correct?

MR. PHILLIPS: That is correct.

MR. STEIN: Can you describe the history that led to the creation of your office?

MR. PHILLIPS: The history is that the Pennsylvania Crime Commission was engaged in a lengthy investigation of corruption within the Philadelphia Police Department and they issued a report in March of 1974. And one of the recommendations they made was that a Special Prosecutor's Office be established to investigate and prosecute police corruption in Philadelphia. This was the same recommendation that the Knapp Commission in New York made that resulted in a Special Prosecutor's office being established there.

MR. STEIN: In the past year you have built up a staff of lawyers and investigators. Can you describe the organization of your office, the number of people you have, and the experience level of the people?

MR. PHILLIPS: Yes. We have 12 attorneys, plus myself. I have a chief investigator, plus 11 other investigators. I have an accountant, a chief accountant, plus one full-time accountant and four or five part-time accountants. And I have an administrative officer.

The experience of the attorneys is that they are young attorneys, very similar to what you heard from Mr. Thompson and what was my experience in New York, attorneys who are interested in doing trial work and doing public service work. They range in experience from one year out of law school for two of the attorneys, to seven years out of law school for one, but generally it is four or five years out of law school.

The investigators were selected from various sources and were hired by my former chief investigator who has since died.

MR. STEIN: Simultaneously with the build-up of your office in 1974, the debate was ongoing as to the new statute which has now been signed into law, and you took an active role in opposing the statute; is that correct?

MR. PHILLIPS: Yes, I did.

MR. STEIN: You also at the time in 1974 obtained some electronic surveillance equipment for your office; is that correct?

MR. PHILLIPS: Yes, we did.

MR. STEIN: And that equipment was turned back to the state upon enactment of the law?

MR. PHILLIPS: Yes, it was.

MR. STEIN: So you now have no electronic surveillance equipment available to you?

MR. PHILLIPS: That is correct.

MR. STEIN: Can you describe the means of investigation you have been pursuing in corruption cases?

MR. PHILLIPS: Well, with respect to public official corruption we have used the grand jury extensively and its subpoena power to obtain records and documents from companies or individuals about which there have been allegations that they have been paying off public officials.

And we have also been using the power to compel testimony through the grant of immunity.

We have been using informants; we have been using undercover agents on certain occasions, and surveillance.

But it is very difficult to detect and investigate ongoing corruption without the ability to use wiretap or one-party consensual monitoring. With respect to past acts of corruption and particularly official corruption as opposed to police corruption, it is somewhat easier or can be done through the grand jury because there is a greater likelihood of records and documents that can be traced and lead to the corrupt transaction.

MR. STEIN: You distinguish, then, between investigations of corruption involving professional criminals and gambling and narcotics and the white-collar-official type of corruption?

MR. PHILLIPS: Yes. There is a distinction with respect to white collar corruption, paying off to get contracts with the city, kick-back contracts—I said the creation of the office was based on the recommendation of the Crime Commission to investigate police corruption. Approximately one month after the office was created we were assigned by the Attorney General to staff a grand jury that was impaneled to investigate official corruption generally in the City of Philadelphia and this is how we got into white collar areas of corruption, the typical type being kick-backs on contracts with the city.

In this area it is possible to investigate past acts of corruption by getting the books and records of the company and having our accountants look through them to see where the generation of cash is reflected.

MR. STEIN: Your investigations, I know, are ongoing. Can you talk about a measure of success in the area of investigating police corruption or gambling?

MR. PHILLIPS: We have had real problems as far as investigating police corruption and particularly ties into gambling, particularly because of the inability to engage in wiretapping and one-party consensual monitoring. We have had allegations that police officers were receiving payoffs from gamblers in certain bars. We have been able to corroborate that police officers were meeting in rooms with alleged gamblers, but being unable to bug the room, we have been unable to pursue those investigations.

MR. STEIN: Does that hold true in the area of narcotics as well?

MR. PHILLIPS: I think to a lesser degree, because gambling is by and large conducted to a great extent on the telephone and in the process of investigating major gamblers through wiretapping you can also find out corruption situations.

Narcotics is, to a lesser degree, engaged in on the telephone, and particularly less in terms of the corruption aspect.

Narcotics does not involve as much wholesale corruption as gambling does. Narcotics corruption involves, I think, more specifically one or two individual police officers here and there.

MR. STEIN: Do you interpret the Pennsylvania statute to mean that you cannot accept evidence of lawful wiretaps from Federal or other jurisdictions?

MR. PHILLIPS: Yes. We have done some research on that, although I don't think—to my knowledge, at least—in Pennsylvania there is any

definitive case law on the subject. I would be very reluctant to use specifically in evidence wiretaps or one-party consensual monitoring that would be a violation of the Pennsylvania law.

I do not think, however, that it would be a violation of the law or taint a subsequent prosecution if information were merely turned over to you that was obtained through illegal wiretapping and you followed it up.

MR. STEIN: Finally, in your investigations into corruption both of political officials and of police, have you come across instances of illegal wiretapping?

MR. PHILLIPS: No, we haven't. There was one very celebrated instance before our office was established in 1972, when certain members of the state police were found to have been illegally bugging a motel of other state police who were engaged in a police corruption investigation. That case resulted in the dismissal of certain state police officers as well as the head of the state police.

Criminal charges were brought, but they were dismissed at a preliminary hearing held by the local magistrate.

MR. STEIN: Do you believe the enactment of an authorization for lawful wiretaps by police and law enforcement personnel would affect illegal wiretapping in any way?

MR. PHILLIPS: No. I know the argument has been made that it would increase the chances of illegal wiretapping to legalize wiretapping. But, as I indicated in my formal statement, my recommendation would be that a panel of judges be established that would be the only judges that could issue court orders for wiretaps, and that any instance of illegal wiretapping, first of all, would be made a felony with a severe penalty and be tried by the Attorney General's Office in front of one of those judges. I think that could conceivably act as as good a deterrent as you could have against illegal wiretapping.

MR. STEIN: That concludes the staff questioning.

MR. REMINGTON: Chief Andersen.

CHIEF ANDERSEN: I have no questions.

MR. REMINGTON: Mr. Blakey.

PROFESSOR BLAKEY: Mr. Phillips, you said at the end of your statement you would make some amendment to the Federal statute. And I understand one of the amendments would be that you would have a panel of Federal judges approving taps rather than a single Federal Judge.

MR. PHILLIPS: Yes.

PROFESSOR BLAKEY: Do you think that is really a proper allocation of judicial manpower? You don't have to have three Federal Judges to approve an arrest. Why should you have to do it for a wiretap?

MR. PHILLIPS: I am not suggesting that all the judges on the panel have to approve the wiretap.

PROFESSOR BLAKEY: I am saying why have a three-judge panel to do it?

MR. PHILLIPS: I am not advocating a three-judge panel to do it. I am advocating there be a panel of judges from which one could be selected.

PROFESSOR BLAKEY: I'm sorry. I misunderstood your statement. What you are suggesting is that the Chief Judge of the United States or Chief Judge of the Circuit or of the District set three designated people.

MR. PHILLIPS: I am not advocating this for the Federal law. I am only advocating this for the Pennsylvania State law. I think the Federal law is fine as it is. I have no problem with it.

PROFESSOR BLAKEY: It is obvious I misread your statement. I'm sorry.

MR. REMINGTON: You state the proposal of a panel of judges for Pennsylvania is to prevent judge-shopping?

MR. PHILLIPS: Yes, it is to prevent judge-shopping and I think, to be frank, the quality of the judges in the state courts is such that to really ensure that there be a close scrutiny of the application, the best judges be selected to pass upon it.

PROFESSOR BLAKEY: We had prior testimony before the Commission by the former District Attorney of Philadelphia, Arlen Specter. He indicated his experience in Philadelphia was—and I hope this is a fair description—that he had never seen a case that needed wiretapping to make it. Would your experience correspond to his?

MR. PHILLIPS: My experience with respect to murder cases would correspond to that. But when you are talking of corruption cases, high-level gambling cases, high-level narcotics cases, you can sit back and arrest the street seller or arrest the numbers writer and occasionally make a police corruption case. But if you are going to engage in any creative investigation which is the only way you are going to go after organized crime and corrupt public officials, I think you have to engage in this type of thing.

The prosecutor that takes the attitude that "my job is to take the cases the police department gives me and prosecute them to the best of my ability in court"—fine, wiretapping is not going to increase his performance.

On the other hand, a prosecutor—and I think the prosecutor's function is not that but to engage in investigations himself in conjunction with the law enforcement agencies and it is the creative, imaginative types of investigations that are going to get the corrupt officials and members of organized crime.

PROFESSOR BLAKEY: Are you suggesting Mr. Specter's office didn't include that imaginative, creative kind of investigation of officials?

MR. PHILLIPS: I was in Mr. Specter's office for two years. I graduated from law school in 1966 and spent two years there before going to New York. And I think Mr. Specter's office probably did an aggressive job given what he had knowledge of. But I think that wiretapping, legal wiretapping and electronic surveillance could have given him greater knowledge of what was going on so he could have engaged in much more imaginative and aggressive investigations.

PROFESSOR BLAKEY: Thank you, Mr. Chairman.

The statement Mr. Phillips has made today is comparable to the one he gave before the National Gambling Commission several weeks ago and I was present at that hearing and there were several other people who discussed the Philadelphia situation, and indeed as it turned out discussed wiretapping in the Philadelphia situation, and also particularly discussed gambling enforcement. And I wonder if the staff couldn't arrange to get the testimony of the FBI and the Superintendent of the State Police, the Municipal Judge, and also the other relevant testimony on Philadelphia wiretapping in gambling that was presented to the Gambling Commission incorporated into the record. I think it would be helpful to people who read our record and much of it was directed to the questions you have asked about: Is it worth it in an area like gambling?

MR. REMINGTON: General Hodson, is that possible?

MR. HODSON: If he can identify the witnesses.

STAFF MEMBER: We have already requested it.

PROFESSOR BLAKEY: I wonder if it could be incorporated in the record at this point.

THE STAFF MEMBER: When it is available.

MR. REMINGTON: Then, without objection, it will be incorporated as part of the record at this time and General Hodson and staff will produce that necessary material.

[The Commission on the Review of the National Policy Toward Gambling will publish its final report and all supplementary materials October 1976.]

MR. REMINGTON: If I may, Mr. Phillips, I would like to ask a question I think you have been responding to.

Tomorrow we will hear from a witness who has written in part as follows:

"Wiretapping and bugging are a dirty business and it is now clear that they do not help to solve, even prevent, much crime."

I take it you disagree with that statement?

MR. PHILLIPS: Yes.

MR. REMINGTON: How, in your opinion, do you explain such widely divergent conclusions about whether these methods do in fact help solve and prevent crime? In other words, how can we have apparently able, conscientious people coming to such widely different conclusions on the central question of whether electronic surveillance helps solve crime?

MR. PHILLIPS: Well, I think if you go back 40 years ago or whatever period of time you want to take, when people were starting to recognize that there was organized crime, as it is now known today in this country, and that organized crime was starting to take over a lot of the criminal activities, such as gambling, narcotics, prostitution, and so forth, in this country, and compare it with today, you find that organized crime still has control over a wide segment of the activity that I have just mentioned.

These people then concluded that in light of the fact that wiretapping has been legal and engaged in by the Federal authorities to a great extent and one-party consensual monitoring has as well, therefore there has been no real impact on organized crime and its control over criminal activity.

And that is, I think, what a lot of people point to in support of their argument that the individual right to privacy outweighs society's and law enforcement's right to engage in electronic surveillance.

But I think, on the other hand, it is possible to point to a lot of very significant successful prosecutions that have been successful only because of wiretapping or other electronic surveillance.

And I can point from my own experience, for example, to New York, when I was Chief of the Narcotics Unit there, and we came down with an indictment of some 86 major narcotics traffickers in April 1973, many of whom were considered the top wholesale distributors of heroin in the City of New York, and who would have been virtually untouched but for certain wiretapping that was engaged in to get these people.

And I think there are many other instances that can be pointed to as well, of major organized crime figures that have been prosecuted successfully and are behind bars or have served time because of being able to get to these individuals through electronic surveillance.

And I think that is where you get this divergent view.

I think the argument made by individuals that electronic surveillance of all types ought to be outlawed is the reason that it hasn't had the impact that it should have had on organized crime.

MR. REMINGTON: Would it, in your judgment, be appropriate in illustrating the point that you make, to say that the same thing is true with regard to search for physical evidence, that is, there is no demonstration that Rule 41 has lowered the incidence of crime in this country?

MR. PHILLIPS: I think that the same argument could be made, yes. I know that in other countries, for example—and I know in my work with narcotics enforcement I had sort of envied those countries, such as France and Canada, that had, I believe, what they call writs of assistance that would enable law enforcement officers to engage in a search without having to establish through a court probable cause to get a search warrant, the same amount of probable cause that is required in the United States.

And my information was from people that I talked to that this had a good effect, a large impact on reducing the amount of heroin trafficking in those countries, particularly in France where they were able to bust up some significant laboratories that were responsible for producing substantial quantities of heroin.

MR. REMINGTON: In other words, the point of that testimony is that in your judgment, if the ability to conduct physical searches were broadened, it would impact on the incidence of narcotics violations?

MR. PHILLIPS: I think it probably would, but I would be hesitant to advocate that in light of the fact that a physical intrusion into somebody's house is such that I think in our belief in our freedoms, it ought to require that a judicial stamp of approval be put on only after the law enforcement agent has shown probable cause to go in there to seize the contraband.

MR. REMINGTON: In your judgment, then, can any argument be made in behalf of the authority to conduct a physical search pursuant to judicial authorization that can't also be made in behalf of authority to conduct an electronic surveillance?

In other words, what I am trying to get to is: Can an argument be made supporting the right of law enforcement to conduct, with court approval, a search for physical evidence, and at the same time argue against allowing law enforcement to conduct electronic surveillance pursuant to a court order?

MR. PHILLIPS: Well, I would agree with what I think Mr. Thompson said about the difference between a search which is directed specifically to a house or an individual and only for a specific time, one instance, whereas the interception or the intrusion into a telephone involves a long period of time, overhearing conversations not of just two individuals but as many as 50 or 100 individuals; and

that there ought to be greater safeguards and closer judicial scrutiny over the latter than there should be over the former, in my opinion.

MR. REMINGTON: Is the difference primarily the threat to individual liberties, or is the difference in terms of the necessity for the authority? In other words, I take it what you just said was that you could see the need for more restrictions in the area of electronic surveillance than is needed in the area of physical searches.

What I want to be clear on is: Is that because there is a greater threat to liberty in the instance of the electronic surveillance, or is it because the need to conduct physical searches is much greater than the need to conduct electronic surveillances?

MR. PHILLIPS: No, I think it is because of the greater threat to individual privacy which I really think is what the Fourth Amendment is all about, protecting one's right to be left alone and engage in private conversations with one's close family, one's loved ones, or one's business clients, or whatever.

I think that is the reason.

MR. REMINGTON: While we are trying to personalize this, would you say, given the choice of having one's home searched or being listened to, that it follows it is of less concern to have your home searched than it is to be listened to; that there is a greater threat to liberty in being listened to than there is to being searched?

MR. PHILLIPS: Well, I think that there is probably a greater intrusion in having one's home searched, particularly as I have seen law enforcement agents search a home pursuant to a search warrant, because they really do a job—as they should do.

On the other hand—and with respect to conversing on the telephone, one can always just assume the conversation is being overheard or intercepted and engage in such a way as not to reveal any private or confidential communications but to await seeing the individual in person to do that.

But is it a pain in the neck to have to live under that threat for any length of time and it is an inconvenience as well to have to always worry about whether somebody is listening in to your conversation.

The search, of course, is over with in a matter of hours.

MR. REMINGTON: One final question.

From your experience in law enforcement, do you have a judgment in this country as to whether the costs to individual liberties are threatened more in the area of arresting people or in the area of listening to them? In other words, to clarify the question: If you were to attempt to strengthen protections of liberties of individual citizens, in other

words, start where the need is greatest as between those who are arrested and those who are listened to, where would the need for protection be greatest?

MR. PHILLIPS: Well, with respect to the area of arrest, I am deeply concerned that individual's freedoms are greatly violated when one is arrested for exercising one's religious or political beliefs. In that area I think arrests can far outweigh the interception of conversations with respect to invasion of one's individual rights.

On the other hand, excluding that segment of those types of arrests, I think the overhearing of conversations probably creates a greater intrusion of privacy, intrusion of one's individual freedom.

MR. REMINGTON: All right.

I thank you very much.

Are there other questions?

CHIEF ANDERSEN: No questions.

MR. PHILLIPS: Mr. Chairman, if I could just mention one thing, I noticed when Lt. McFadden was testifying you got into a discussion about the right of police to overhear conversations coming into the police department.

What happened in Pennsylvania was that after the new anti-eavesdropping bill was passed, the Pennsylvania Supreme Court came down with a decision upholding the right in a particular case of the police to record the conversation of an incoming call. And this was under the old law which even then made it a violation of law to record over the telephone, where one party consented, a conversation. And by somewhat convoluted reasoning the court ruled that despite the plain language of the statute, it was okay.

However, in response to that decision and after the bill had been passed and signed by the Governor, the Legislature passed an amendment with very little publicity, where they provided an exception for incoming police calls to be recorded without the consent of the caller.

CHIEF ANDERSEN: Thank you.

MR. PHILLIPS: I just thought I would clear that up.

MR. HODSON: I would like to ask you one question, Mr. Phillips, about illegal wiretapping. You mentioned particularly that the police were wiretapping each other?

MR. PHILLIPS: Yes.

MR. HODSON: Can you tell me from your own knowledge, what is the activity of the FBI in the area of illegal wiretapping? I assumed you were referring to incidents which took place after 1968. Has the FBI been active in investigating illegal wiretapping?

MR. PHILLIPS: The FBI—I really do not know. I think it is unfortunate that the FBI and the United States Attorney did not prosecute that particular incident in 1972 of state police engaging in the illegal bugging of the room. I think that would have been a case that they ought to have—

MR. HODSON: Do you know why they did not?

MR. PHILLIPS: No, I do not.

PROFESSOR BLAKEY: Mr. Chairman, could I ask that a letter be written to the Department to ask why they declined that case and that it be inserted in the record at this point?

MR. REMINGTON: A letter written to—

PROFESSOR BLAKEY: —to the people involved in the case to ask them why they declined.

MR. REMINGTON: And the people involved would be who?

PROFESSOR BLAKEY: I take it the United States Attorney.

MR. PHILLIPS: The United States Attorney for the Eastern District of Pennsylvania.

MR. REMINGTON: All right; without objection that will be done.

[Note: An informal inquiry by the staff disclosed that Philadelphia FBI Agent Jack Howell reported the above incident to First Assistant U. S. Attorney John Sutton, who indicated that his office was not interested in a Federal investigation with a view to Federal prosecution, basically on the grounds that the incident was a local matter and could be handled adequately by local authorities under Pennsylvania law.]

MR. REMINGTON: Mr. Phillips, is there anything else you think we should know today?

PROFESSOR BLAKEY: Mr. Chairman, I have two other questions.

You came in April of '74?

MR. PHILLIPS: Yes.

PROFESSOR BLAKEY: The statute comes in in November of 1974?

MR. PHILLIPS: That is when it was passed by the Senate.

PROFESSOR BLAKEY: And I also understand from the newspapers in Philadelphia that you have had some trouble with your funding from the State Legislature?

MR. PHILLIPS: That is correct.

PROFESSOR BLAKEY: Do you think there is any relationship with your difficulty in getting funding and this legislation and your coming in on an anti-corruption campaign in Philadelphia?

MR. PHILLIPS: I think there probably is. I have been told specifically that—what happened was that the bill came up for a vote in the Senate at the end of November, and it passed. As a matter of fact, two days before it came up for a vote in the Senate, the *Philadelphia Inquirer*—there had been nothing on it up until then—wrote an editorial supporting the bill. It was in response to that editorial I wrote a letter to the *Inquirer*. Two days later the bill passed and I became a sort of front-runner, even in that two-day period, of opposing this particular legislation.

And I have been told that certain Senators were quoted as saying afterwards, after the bill was passed, "That will teach that SOB in Philadelphia, the Special Prosecutor."

PROFESSOR BLAKEY: Thank you very much, Mr. Phillips.

MR. REMINGTON: Mr. Phillips, we very much appreciate your willingness to be with us today. Your testimony was very helpful.

MR. PHILLIPS: Thank you very much.

MR. REMINGTON: I think that is all except to announce that, as you may know, the room is changed for tomorrow and it is 1202 Dirksen Building in the morning and 4200 Dirksen Building tomorrow afternoon.

[Whereupon, at 4:25 p.m., the hearing was adjourned, to reconvene at 9:30 a.m., Tuesday, June 10, 1975]

Hearing, Tuesday, June 10, 1975

Washington, D.C.

The hearing was reconvened at 9:30 a.m., in Room 1202, Dirksen Building, William H. Erickson, Chairman, presiding. Commission members present: William H. Erickson, Chairman; Richard R. Andersen, G. Robert Blakey, Frank J. Remington, Florence P. Shientag.

Staff present: Kenneth J. Hodson, Esq., Executive Director; Michael Lipman, Esq., Milton Stein, Esq., Margery Elfin, Esq.

PROCEEDINGS

CHAIRMAN ERICKSON: Ladies and gentlemen, the Commission will stand convened.

Today we have the benefit of testimony by some of the critics of wiretapping. We will hear from some of the most highly regarded individuals, and those that probably have the greatest expertise in the field of electronic surveillance and have occasion to study this statute that we are attempting to review with an eye towards making revisions, corrections, and with an eye to privacy.

The Honorable Ramsey Clark has been delayed but should be here by approximately 10 o'clock. As all of you know, he is the former Attorney General of the United States.

And our first witness today will be the Honorable Herbert Stern, formerly the U. S. Attorney in Newark, New Jersey.

Following his testimony and that of Ramsey Clark, we will hear from Professor R. Kent Greenawalt of Columbia University, Professor Edith Lapidus of Queens College in New York, Professor Richard Uviller of Columbia University Law School, and Professor Herman Schwartz of the State University of New York.

Some of our witnesses have specific critiques concerning electronic surveillance. Judge Stern, for example, is here to discuss the thesis of some law enforcement authorities that nonconsensual electronic surveillance is unnecessary in investigations of organized political corruption.

Professors Greenawalt, Lapidus, and Uviller have comments on specific aspects of the wiretapping statute which they believe need revision.

On the other hand, Attorney General Clark and Professor Herman Schwartz have broader-based objections as to the use of electronic surveillance. They will present the general case against wiretapping.

Before calling Judge Stern, I would point out to the members of the Commission that the work of the Commission is proceeding towards completion, and as we look at the testimony that has been presented, and will yet be presented in the future, we should give serious consideration to the findings and recommendations that this Commission will make.

And at an early meeting following this meeting, I would hope that all members of the Commission would be in a position to make their specific recommendations and their specific suggestions regarding findings that should flow from the testimony and exhibits that have been offered in connection with this Commission's work.

Our report will be in the state of preparation for a period of months. We will be working on that report, making recommendations, making critiques, if you will, of the work that has been done, but hopefully the work that is put together will suggest by its own terms what can be done to assist in the use of wiretapping as a tool, provided constitutional safeguards are followed, and also in protecting rights of privacy.

I believe before introducing Judge Stern, General Hodson has some matters he would like to put on the record.

MR. HODSON: Mr. Chairman, in preparing for this hearing, we addressed letters with enclosed questionnaires to some 10 organizations and some 20 individuals who appear to have an interest in electronic surveillance, the subject we are studying.

I would suggest that for the record we include a list of those organizations and individuals to whom requests were made for comments, together with a copy of the questionnaire which we submitted to each one of them, and their replies to our letter. I suggest they be made a part of the record.

CHAIRMAN ERICKSON: If there are no objections to that recommendation, the recommendation will be followed. The questionnaire will be filed and made a part of the record, and the answers thereto are also included as part of the record of this Commission.

[The documents referred to follow.]

QUESTIONNAIRE:	ELECTRONIC	SURVEILLANCE
CRITICS		

1. Please describe your background, interest in electronic surveillance legislation, and experience with the topic.

2. Do you believe non-consensual electronic surveillance is necessary for the investigation of ongoing criminal conspiracies or organized criminal activity? Is it necessary in the investigation of narcotics rings? Gambling rings? Are alternative investigative means such as use of informants or undercover agents preferable to electronic surveillance under court order?

3. Is the list of crimes for which court-ordered electronic surveillance may be authorized under Federal law adequate? Should it be more limited? Should court-ordered electronic surveillance be permitted for investigation of violent crimes such as murder, kidnapping, terrorist attack, insofar as the crimes might be solved or prevented through non-consensual surveillance?

4. Should electronic surveillance upon consent of one party to the conversation be proscribed? If so, should there be an exception authorized for law enforcement purposes? Should it be subject to court-order? Should it be subject to any type of regulation or reporting?

5. Is responsibility for authorization of an application for court-ordered electronic surveillance properly placed with State and local prosecutors, as well as with the United States Attorney General or any Assistant Attorney General designated by him? Is the Federal system too centralized? Are the State systems too decentralized?

6. Is there a role for greater judicial supervision during the course of a court-ordered electronic surveillance? Should progress reports to the issuing Judge be required by law? Is there need for the provision authorizing emergency interceptions? Should emergency interceptions be subject to prior judicial approval?

7. Is the initial 30 day authorization period for a wiretap or "bug" too lengthy? What would be an adequate period for initial electronic surveillance? Should a mandatory limit to the number of times an electronic surveillance order may be extended be set forth in the statute, even if extended conspiracies are involved? Is the provision permitting postponement of notice of the electronic surveillance to persons intercepted necessary, so that an extensive investigation may continue without exposure?

8. Should standards for minimization of electronic surveillance interceptions be set forth in the statute? What minimization standards would you suggest?

9. Should statutory distinctions be made between wiretapping a telephone and "bugging" a premises? Should an applicant for an order to bug a premises be required to specify whether a breaking and entering is required to plant the "bug" and to obtain explicit court authorization for this procedure?

10. Is privacy best protected by storage under seal of tapes obtained through electronic surveillance for a ten-year period as now required? Can and should a means be devised to maintain information on criminal activities obtained through electronic surveillance permanently, while protecting non-criminal information from disclosure? Could the tapes be destroyed earlier than 10 years if the law provided for notice to all parties and a hearing?

11. Do you have any suggestions as to what information should be included for publication in reports to the Administrative Office of the United States Courts concerning each wiretap? Are they necessary? What other facts should be reported? Consensual taps? Illegal taps?

12. Is the Federal law effective in its prohibition of manufacturing, distribution, possession and advertising of wire or oral communication interception devices for purposes not related to the needs of a communications common carrier or of law enforcement? Should manufacturers of such equipment be subject to licensing? Do you have any other suggestions for stemming proliferation of this equipment? There have been a number of reports in the media of illegal wiretapping by local police (Houston, Williamsport (PA), Cedar Rapids (Ia), NYC. Do you have any views as to the competency of the FBI to investigate such cases? Is there an alternative?

13. Is the exception granted to communications common carriers to intercept communications insofar as necessary to the protection of the rights or property of the carriers of such communications too broad? Should the statute explicitly proscribe interception of telephone communications of employees in an office by the employers? What of companies which conduct most of their business by telephone, such as airlines reservations? Is there any expectation of privacy in communications by an employee on a business telephone? If so, how should that expectation be defined?

Organizations

American Bar Association, Washington, D.C.

American Civil Liberties Union, New York, N.Y.

Americans for Effective Law Enforcement, Evanston, Illinois

Association of the Bar of the City of New York, New York, N.Y.

Association of Trial Lawyers of America, Cambridge, Mass.

National Association of Attorneys General, Raleigh, North Carolina

National Association of Criminal Defense Attorneys, Austin, Texas

National District Attorneys Association, Chicago, Ill.

National Lawyers Guild, Electronic Surveillance Project, San Francisco, Calif.

National Legal Aid and Defender Association, Washington, D.C.

Individuals

Professor Frank Askin, Rutgers University, Newark

William J. Bender, Esq., Rutgers University, Newark

Professor James G. Carr, University of Toledo College of Law

Hon. Ramsey Clark, New York, N.Y.

Professor Samuel Dash, Georgetown University Law Center

Mr. Fred East, Office of the District Attorney, Los Angeles, Calif.

Professor B. F. George, Jr., Wayne State University

Professor R. Kent Greenawalt, Columbia University

Philip J. Hirschkop, Esq., Alexandria, Va.

Professor Fred E. Inbau, Northwestern University

Professor Edith Lapidus, Queens College, N.Y.

Jack J. Levine, Esq., Philadelphia, Pa.

F. Russell Millin, Esq., Kansas City, Mo.

Hon. Frank Rizzo, Mayor, Philadelphia, Pa.

Charles Rogovin, Esq., Newton, Mass.

Steven Sachs, Esq., Baltimore, Md.

Henry Sawyer, Esq., Philadelphia, Pa.

Professor Herman Schwartz, S.U.N.Y., Buffalo

Professor Louis B. Schwartz, University of Pennsylvania

Professor Ralph S. Spritzer, University of Pennsylvania

Judge Herbert Stern, Newark, N.J.

Professor Telford Taylor, Columbia University

Professor Michael E. Tigar, UCLA

Professor H. Richard Uviller, Columbia University

Columbia University in the City of New York
New York, N.Y. 10027

SCHOOL OF LAW

435 West 116th Street

May 8, 1975

National Commission for the Review of
Federal and State Laws relating to
Wiretapping and Electronic Surveillance
1875 Connecticut Avenue, N.W.
Washington, D.C. 20009

Attention: Kenneth J. Hodson, Executive Director

Dear Mr. Hodson:

I have reviewed with interest the questionnaire submitted with your letter of April 30th. On some of the points I have strong views, while others are remote to my experience and reflection. So I will answer some of the questions and pass over those concerning which I do not think I have anything to contribute.

1. In private practice I have occasionally touched Fourth Amendment problems. In conducting constitutional law classes I have paid a good deal of attention to this subject. See also the first part of my book *Two Studies in Constitutional Interpretation* (1969), which deals in part with electronic surveillance.

2. My answer here should be read in conjunction with my answer to No. 9. Assuming that no clandestine entry is involved, I believe that electronic surveillance is helpful, if not necessary, for the investigation of the kind of crimes referred to in your question.

3. I believe that the list of crimes authorized in Federal law is much more than adequate. Electronic surveillance involves a serious invasion of privacy and its use should be restricted to serious crimes.

4. I do not believe that it is necessary to prohibit surveillance where one of the parties has consented, though there may be particular circumstances where I would take another view.

6. I do not place a high value on judicial supervision in this area, because the problems seem to me much more prosecutorial and administrative than judicial.

9. By all means an applicant for a court order should be required to specify whether the surveillance involves a clandestine entry. In my view, such a procedure should virtually never be authorized. Certainly, it should not be used to gather evidence for criminal prosecution. There may be circumstances where it would be justified for national intelligence or security reasons. But it is an anomalous, dangerous and, in my view, unconstitutional procedure which should have no place in law enforcement.

Very truly yours,

[Signed] Telford Taylor

Henry Wade

District Attorney

Dallas County Government Center
Dallas, Texas 75202

June 9, 1975

Mr. Patrick F. Healy, Executive Director
National District Attorneys Association
211 East Chicago Avenue, Suite 1515
Chicago, Illinois 60611

Dear Mr. Healy:

Enclosed please find answers to the questionnaire sent to our office concerning wiretapping and electronic surveillance.

Mr. Wade asked me to respond for our office as I have had some exposure to the issues involved. If I can be of further service, please let me know.

Sincerely,

[Signed] J. R. Ormesher
Assistant District Attorney
Dallas County, Texas

JRO/ss
Encl.

TO: Mr. Patrick F. Healy, Executive Director National District Attorneys Association

FROM: J. Russell Ormesher

RE: Federal and State Laws Relating to Wire Tapping and Electronic Surveillance

DATE: June 9, 1975

1. I work as the Chief Felony Prosecutor for the District Attorney's Office in Dallas, Texas and have been employed as a prosecutor with that office for eight years. I have worked also as Executive Director of the Texas Law Enforcement Legislative Council and as such have actively sought the adoption of an electronic surveillance enabling statute for the State of Texas, which Texas presently does not have. In that connection I have found it necessary to study the Federal statute and to do considerable reading on the topic. Also I have had opportunity to talk to various law enforcement officers around the State of Texas concerning their views on electronic surveillance and the need for a state statute in Texas.
2. (a) I strongly believe that non-consensual electronic surveillance is necessary for the investigation of criminal conspiracies and organized crime activity.
(b) Electronic surveillance is needed for use against narcotics rings and gambling rings.
(c) I believe that alternative investigative means are preferable to electronic surveillance under court order in certain circumstances. However, it has been our experience locally that use of informants and undercover agents is of limited effect and when used heavily become less effective the longer the procedure is used and therefore there must be a supplement to these activities and the supplement which I see as being strongly necessary is that of electronic surveillance under the court order.
3. (a) I believe the list of crimes for which court ordered electronic surveillance may be authorized under federal law is adequate.
(b) I would not limit this list any further.
(c) I would not eliminate the use of electronic surveillance as a tool for solving the offenses of murder, kidnapping and terrorist attacks simply because they might be solved or prevented through other types of surveillance.
4. (a) Electronic surveillance upon consent of one party to the conversation should not be proscribed. If a person publishes his thoughts to an individual, he should have no expectation of privacy and should not be heard to complain if the conversation is recorded.
(b) If such surveillance were proscribed most certainly there should be an exception for law enforcement purposes including the right of prosecutors to engage in such type of surveillance. This is particularly needed as the American Bar Association is making attempts to prohibit attorneys from engaging in recording of conversations with other parties without telling them that the conversation is being recorded. This in my opinion would be adverse to the prosecutors right to adequately prepare his criminal case.
(c) No, this type of surveillance should not be subject to court order.
(d) This type of surveillance should not be subject to regulation or reporting. I do not perceive the activities set out in question four as truly being surveillance. These activities merely seek to preserve what an individual is hearing and should not be subject to the protection of use of warrants.
5. (a) I believe the responsibility for authorization is properly placed with state and local prosecutors as well as the United States Attorney General.
(b) I do not believe that the federal system is too centralized.
(c) Nor do I believe that the State systems are too decentralized.
6. (a) I do not believe that the judiciary needs to take a stronger role in supervision of court ordered electronic surveillance than that required in the federal statutes.
(b) Yes, progress reports should be made to the issuing judge.

- (c) Yes, there is a need for the provision authorizing emergency interceptions.
7. (a) The initial 30 day authorization is not too lengthy.
 (b) I believe that the 30 day period is adequate.
 (c) I do not believe there needs to be a mandatory limit on the number of times an electronic surveillance order may be extended. This is a matter that should be left to the discretion of the court.
 (d) The provision permitting postponement of notice of the electronic surveillance is absolutely necessary in some situations.
8. (a) I do not believe standards for minimization should be set forth in the statute. If the requirements of probable cause are meant, I do not feel that this type of investigative tool should have any more limitations placed on it than, for example, the search of an individual's home.
9. (a) I do not believe that statutory distinctions need to be made between wire tapping a telephone and bugging a premises other than those suggested in the following answer.
 (b) An applicant for an order to bug premises should be required to specify whether breaking and entering is required and should obtain explicit court authorization for the procedure.
10. (a) I have no disagreement with the storage for ten year period as now required other than as set out in the following answer.
 (b) Means should be devised to maintain information on criminal activities obtained through electronic surveillance permanently. These means should prevent dissemination of non-criminal information.
 (c) There should be a procedure provided for the destruction of the tapes where notice is made to all parties and a hearing procedure is provided.
11. (a) I have no suggestions for additional data.
 (b) I believe these reports are necessary as a means of evaluating the effectiveness of the use of electronic surveillance and of monitoring the use of this activity.
 (c) I have no suggestion concerning what other facts should be reported.
 (d) I would not require the reporting of consensual taps.
 (e) Information concerning illegal taps should be gathered.
12. (a) I do not possess adequate data or experience in this area to form an adequate opinion.
13. (a) I am not familiar with the activities of communications common carriers and have no opinion as to the breadth of the exception granted to them concerning intercepting communications.
 (b) I do not believe that the statute should proscribe interception of telephone communications of employees in an office by the employer.
 (c) My answer would be the same concerning companies which conduct most of their business by telephone.
 (d) I believe there is an expectation of privacy in communication by an employee on a business phone but I do not believe that this expectation should run as to the employer who provides the office and telephone that is being used.
 (e) The expectation should be defined in a manner that would eliminate the employer from the field of expectation.

STEPHEN J. McEWEN, JR.

District Attorney
 Delaware County Court House
 Media, Pennsylvania 19063

June 30, 1975

FROM: STEPHEN J. McEWEN, JR., DISTRICT ATTORNEY
 TO: NATIONAL DISTRICT ATTORNEYS ASSOCIATION

RE: ELECTRONICS SURVEILLANCE QUESTIONNAIRE

- For the past seventeen years I have practiced the profession of the law, a significant part of that time having been spent in the trial of criminal cases, representing defendants for the first few years in the office of the Philadelphia Public Defender and subsequently representing defendants in my private practice and for the past eight years having served as District Attorney of Delaware County, Pennsylvania, a jurisdiction of more than 600,000 people and a staff of approximately 30 Assistant District Attorneys.
- My basic belief is that there should be a general prohibition of non-consensual electronic surveillance with the sole exception being where matters of national security are involved. Almost any method of gathering information is preferable to electronic surveillance. All of the answers to this question are based upon the premise that my desire to generally prohibit all electronic surveillance is not acceptable and, therefore, it is necessary to make some adjustments in my point of view. Therefore, a mention of any preference or any alternative is simply an expression of my view in light of the fact that a general prohibition is not accepted.
- In my opinion 18 U.S.C. 2516 should be limited to subparagraph (a) which deals with national security and the use of electronic surveillance for any other purpose should be prohibited, although would permit such surveillance in connection with the crimes of murder and terroristic attack but would restrict the use of such information gained from such surveillance to investigative purposes and would not permit such information to be used as evidence in any legal proceeding or prosecution.
- Generally, electronic surveillance upon consent of one party to the conversation should be prohibited, but an exception should be permitted in the case of a lease or fire communication centers since it is desirable for the personnel of such an agency, while acting in the performance of their duties, to record conversations to preserve their accuracy. This exception should be limited to situations where the individual would no longer have a reasonable expectation of privacy and should not be extended to any conversation to which a law enforcement official is a party but should be limited to those conversations where the assistance of law enforcement or fire fighting or prevention agencies render assistance (current Pennsylvania law, 18 P.S. Section 5705, prohibits the recording of such conversations without a Court Order. This is an anomalous situation which deserves prompt statutory amendment).
- Since I start from the premise that the use of electronic surveillance should be strictly limited, the fewer officials that have power to authorize an application the better; therefore, I consider the federal limitation proper, and would limit the state power to authorize to the Attorney General or a specifically designated Assistant Attorney General.
- 18 U.S.C. 2518 (b) should be amended to read . . . the Order *must* require reports . . . at such intervals as the judge may require, but not later than 15 days after the issuance of the Order and every 15 days thereafter for as long as the surveillance continues. Emergency situations should also require prior judicial approval.
- In my opinion an unsupervised 30 day authorization is too lengthy, but could be cured by a system of interim reporting. There should be stricter criteria set for the approval of extensions, quite possibly it would be preferable to require that all extensions be approved by the majority of a three judge panel. Since the invasion of the privacy of the individual is the main offense, delay in giving him notice would not substantially add to the infringement of his rights.
- Yes, I agree with the Court of Appeals for the District of Columbia, "Where the probability is high that persons not under investigation will be using the tapped telephone or that

content of calls will not pertain to subject matter of investigation, Government should adopt procedure to limit interception of those calls", *U.S. vs. James*, 494 F2d 1007. The exact method to be used remains to be discussed and considered.

9. There should be a distinction made between the two methods of surveillance in that two separate zones of privacy are involved, and if a breaking and entering is required the Court should be so informed in order that it can give the proper weight to that particular intrusion into the Fourth Amendment rights of the subject.

10. The sooner that tapes containing nonessential information are destroyed the better and once any tape has satisfied its investigative function, it should be destroyed. It strikes me that rather than have the government be permitted to destroy tapes only after notice and hearing, it is by far preferable to reverse the onus and then only provide for tapes to be destroyed unless and until the government secures Court approval, after notice and hearing, or a longer period of preservation.

11. I would suggest that the report include the number of conversations that were nonessential to the investigation, and a statement as to what precautions were being used to avoid the interception of these nonessential calls.

12. It is obviously not wholly effective, as this type of activity continues. The licensing of manufacturers and distributors of such equipment, along with the establishment of a separate agency to enforce the regulations and prosecute the violators might be more effective, but the cost has to be weighed against the potential benefit.

13. *Common Carriers*—In my opinion there should be a stricter limitation placed on the type of disclosure and a very high minimum fine if found to be abusing the privileged exception.

Employees—Even though the employee would no longer have an expectation of privacy, the other party to the conversation would, and any such recording would violate that expectation.

Airlines, etc.—These companies have sound economic reasons for recording conversations, but in the general interest of protecting the privacy of all, these economic interests must be subordinated to the common good.

Employee-Business phone—The employee may not have an expectation of privacy but the other party to the conversation does and, therefore, no interception should be permitted.

Every man has a basic right as a person and an individual to anticipate that any conversation in which he engages will not go beyond the immediate reach of his voice but if he is aware of the likelihood or possibility of interception, such as communications by radio, that individual can be assumed to have waived his right to privacy.

State of Louisiana
DEPARTMENT OF JUSTICE

William J. Guste, Jr.
ATTORNEY GENERAL

7th FLOOR
2-3-4 LOYOLA BUILDING
NEW ORLEANS 70112

June 27, 1975

Mr. Kenneth J. Hodson, Executive Director
National Commission for the Review of
Federal and State Laws Relating to
Wiretapping and Electronic Surveillance
1875 Connecticut Avenue, N.W.
Washington, D.C. 20009

Dear Mr. Hodson:

My office has received a copy of the Commission's Electronic Surveillance Questionnaire from the Committee on the Office of Attorney General.

Pursuant to their invitation and under my direction, the Organized Crime and Racketeering Section of the Louisiana Department of Justice has drafted our response, which is enclosed herewith for your convenience and perusal.

If we may be of any further assistance to you or the Commission, please do not hesitate to call on us.

Very truly yours,

[Signed] William J. Guste, Jr.
Attorney General
State of Louisiana

Encl.

National Association of Attorneys General
Committee on the Office of Attorney General
1516 Glenwood Avenue
Raleigh, North Carolina 27608

TO: Organized Crime Control Contacts
FROM: Richard Kucharski, Organized Crime Control Coordinator
SUBJECT: NATIONAL WIRETAP COMMISSION QUESTIONNAIRE
DATE: May 20, 1975

Enclosed you will find a letter and a questionnaire from the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance. The Commission has asked COAG to distribute these materials and invite your comments on the federal electronic surveillance law.

If you feel it is appropriate, please forward these materials to your Attorney General for comment.

RESPONSE TO ELECTRONIC SURVEILLANCE QUESTIONNAIRE

1. The Organized Crime & Racketeering Unit of the Louisiana Department of Justice was established two years ago. Its primary purpose is the gathering of intelligence data relative to certain organized crime activities, including gambling, prostitution, narcotics, extortion, and various frauds. Staffed with six attorneys, the Unit is also capable of bringing certain cases to trial in cooperation with various district attorneys throughout the State. Consequently, we have great interest in electronic surveillance legislation, and at least one case brought to trial by this Unit dealt extensively with the law related to electronic surveillances.

It should be noted at the outset that while L.R.S. 14:322 generally bestows the power of wire interception on law enforcement agencies throughout the State, the Section does not conform to the guidelines set out in Title 18:2516 of the United States Code. Accordingly, Louisiana has no general wiretap law. The only legal basis for obtaining wiretap evidence in this State is through the judicially established consensual eavesdropping rules laid down most recently in *United States v. White*, 401 U.S. 745, 91 S.Ct. 1122, 28 L.Ed. 2d 453 (1971). There is no outstanding authority for non-consensual electronic surveillance.

2. We believe that non-consensual electronic surveillance is necessary for the investigation of ongoing criminal conspiracies or organized criminal activity, be it narcotics rings, gambling rings, or whatever. While the use of informants, undercover agents and consensual eavesdropping do provide a means for obtaining some of the evidence which may also be obtained by non-consensual eavesdropping, we consider them to be less effective against sophisticated criminal types who are inclined to withhold their activities from detection through normal police procedures. Non-consensual eavesdropping appears to be the more efficient, effective, and safest means of obtaining the necessary evidence to investigate and prosecute criminal matters, particularly in situations involving prospective offenses such as extortion and bribery.

3. The list of crimes for which court-ordered electronic surveillance may be authorized under federal law is adequate. Certainly, it should not be more limited. We specifically note that paragraph 2 of Section 2516 of Title 18 provides what appears to be an appropriate catch-all for all violent crimes, and we feel that it should be used accordingly.

4. Electronic surveillance, upon the consent of one party to the conversation should not be proscribed. This is the only means by which such evidence presently may be obtained in Louisiana. Further, we note that Mr. Justice White, in his opinion in the case of *United States v. White, supra.*, dealt with the policy considerations behind permitting the use of consensual eavesdropping evidence. Generally, he observed that a party to the conversation could remember it or make notes or do whatever else that would be necessary in order for him to render an accurate account of the conversation. He noted that tape-recording the occurrence is the most accurate means of reproducing the conversation. Assuming that a satisfactory chain of evidence can be established, the only disadvantage to the defendant, against whom evidence obtained during a consensual eavesdropping is introduced, is that his lawyer cannot cross-examine the other party on the accuracy of his recollection of the conversation. Accordingly, we do not believe that such surveillance should be subject to a court order, nor do we believe that it should be subject to any type of regulation or reporting.

5. The responsibility for authorization of an application for court-ordered electronic surveillance is properly placed with state and local prosecutors, as well as the United States Attorney General or any Assistant Attorney General designated by him. We note that since the legal procedures in obtaining a court-ordered surveillance are quite similar to those involved in obtaining a search warrant, the prosecutor is the only authority equipped to make application for such order.

6. We do not believe that greater judicial supervision during the course of a court-ordered electronic surveillance is needed. Progress reports to the issuing judge should not be required by law. Generally, we agree that there is need for the provision authorizing emergency interceptions, but that such emergency interceptions should be subject to some sort of judicial approval to insure the Fourth Amendment rights of the potentially aggrieved person.

7. We agree with the thirty-day authorization period as set out in the present wire-tap law. Each case necessarily rests on its own facts. Consequently, it would appear unnecessary and unwise to set a mandatory limit as to the number of times an electronic surveillance order may be extended. Likewise, the facts of any given case may demand that notice of the electronic surveillance to persons intercepted be postponed so that the investigation may continue without exposure.

8. Standards for minimization of electronic surveillance should not be set forth in a statute. Rather, we deem it more appropriate for the issuing court to do so in its order. In this way the scope of each surveillance could be tailored to the given facts of the case.

9. Statutory distinction should not be made between wire-tapping a telephone and electronic surveillance of a premises. We note that this distinction was specifically rejected by the United States Supreme Court in *Katz v. The United States*, 389 U.S. 347 88 S.Ct. So. 7, 19 L.Ed.2d 576 (1967). Accordingly, we believe that the same rule should apply to intercepted communications whether they be by telephone tap or by electronic surveillance of a premises. However, where entry into the premises is desired, a provision to that effect should be contained in the court order.

10. We believe that privacy is adequately protected by the storage under seal of electronic surveillance tapes for a ten-year period as presently required by the law. We see grave dangers in permanently maintaining and collating data obtained through electronic surveillances; however, we see no reason why the

tapes should not be destroyed earlier than ten years if the law provided for notice to all parties of a hearing.

11. We do not believe that any information obtained from any wiretaps should be included in reports to the administrative office of the United States Courts. For statistical purposes only, we would recommend that the office be informed every time a non-consensual tap has been completed.

12. The federal law appears to be relatively effective in its prohibition of manufacturing, distribution, possession and advertising wire or oral communication interception devices for purposes not related to the needs of a communications common carrier or of law enforcement. However, it appears to us that the statute is limited inasmuch as its scope is limited to interstate commerce, and further regulation would appear to be necessary at a state level. We know of no reason which would lead us to believe that the FBI is not equipped to investigate cases of illegal wire-tapping by local police.

13. We do not believe that the exception granted to communications common carriers to intercept communications insofar as is necessary to the protection of the rights or property of the carriers of such communications, is too broad. The statute wisely draws a distinction. It provides the exemption where the information is received in the ordinary course of conducting necessary business activities. In other words, information which appears to come to the carrier purely coincidentally is not covered. On the other hand, it proscribes a systematic scanning of the communications network for the sole purpose of gaining information relative to crime.

Generally, our office supports the statement of Henry E. Petersen, Assistant Attorney General, Criminal Division, before the Sub-Committee on Courts, Civil Liberties in the Administration of Justice Committee on the Judiciary House of Representatives concerning wire-tapping and electronic surveillance, dated April 26, 1974. That statement points out that much of Title III was drafted to meet the constitutional requirements for electronic surveillances as laid down in various decisions of the United States Supreme Court.

In commenting on the effectiveness of electronic surveillance, Mr. Petersen said:

We maintain that electronic surveillance techniques are, to date, the most effective method to bring criminal sanctions against organized criminals, and are indispensable in developing witnesses with corroborating testimony, and generally in providing a useful tool in the evidence-gathering process. The Department's most notable success with the use of electronic surveillances has been against organized crime controlled gambling enterprises. However, surveillances have also proved extremely useful in detecting and arresting violators of the other crimes listed in Section 2516 of Title 18. Our successes require us to recommend that Title III remain unchanged.

Harry F. Connick
District Attorney of New Orleans

State of Louisiana

July 14, 1975

Mr. Patrick F. Healy, Executive Director
National District Attorneys Association
211 East Chicago Avenue
Chicago, Illinois 60611

Dear Pat:

Enclosed you will find my response to the questionnaire pertaining to wiretapping and electronic surveillance.

Sincerely,

[Signed] Harry F. Connick
District Attorney

Enclosure

(1) Presently, District Attorney of New Orleans, the largest urban area in the State of Louisiana. Formerly, Chief of Criminal Division, U.S. Attorney's office, Eastern District of Louisiana. Formerly, Chief of Criminal Division of Legal Aid Society-New Orleans.

- (2)
- (a) Yes.
 - (b) Yes.
 - (c) Yes.
- (d) Electronic surveillance is preferred because there is no credibility problem (as is the case with informants) and there is no elusive memory problem (as is the case with undercover agents testifying about specific words used in a conversation that took place months before trial).

- (3)
- (a) 18 U.S.C. Section 2516 is comprehensive enough.
 - (b) No.
 - (c) Statistics show that most murders are committed in the heat of passion among people who know one another and many other murders are committed in the course of other criminal activities (armed robberies, rapes, burglaries, etc.) that don't require any degree of planning. It is unlikely that electronic surveillance will enable law enforcement officials to prevent these crimes. On the other hand, once the suspects have been narrowed down, electronic surveillance may assist the police in solving these crimes.

- (4)
- (a) The answer is, emphatically, no, because if this kind of legislation passes into law, it would wipe out the "misplaced confidence" rule established by the United States Supreme Court. See *United States v. White*, 401 U.S. 745 (1971); *Hoffa v. United States*, 385 U.S. 293 (1966); *Lewis v. United States*, 385 U.S. 206 (1966); *Osborn v. United States*, 385 U.S. 323 (1966); and *Lopez v. United States*, 373 U.S. 427 (1963).

(b) If the kind of law proposed in the first sentence of paragraph 4 passes into law, the second sentence would kill it, and the state of the law would be the same as if there were no such law to begin with.

(c) In *Osborn*, supra, there was a prior judicial order authorizing the type of electronic surveillance conducted. But it seems senseless as long as one party consents thereto.

(d) The best idea contained in paragraph 4 is the last sentence. As long as one party consents, there shouldn't be any regulations imposed.

- (5)
- (a) Yes. Whoever has jurisdiction over the criminal activity under investigation should have the authority to approve wiretap applications prior to making application for judicial authority.

(b) Congress, in 18 U.S.C. Section 2516(1), made a preliminary approval of submission of wiretap applications a central safeguard in preventing the abuse of this means of investigative surveillance and intentionally restricted the category of federal officials who could give such approval to only the Attorney General himself or any Assistant Attorney General he might specifically designate for that purpose. Failure to secure approval of one of these individuals prior to making application for judicial authority to wiretap renders the court authority invalid and the interception of communications pursuant to that authority "unlawful" within the meaning of 18 U.S.C. Section 2518(10)(a)(i).

Failure to correctly report the identity of the person authorizing the application, however, when in fact the Attorney General has given the required preliminary approval to submit the application, does not represent a similar failure to follow Title III (of the Omnibus Crime Control and Safe Streets Act of 1968, 82 Stat 211-225, 18 U.S.C. Sections 2510-2520)'s precaution against the unwarranted use of wiretapping or electronic surveillance and does not warrant the

suppression of evidence gathered pursuant to a court order resting on the application. *United States v. Chavez*, 416 U.S. 562 (1974).

The problem rests with centralization, rather than decentralization, since it is the judicial officer who has the last word on whether or not wiretapping or electronic surveillance is authorized.

- (6)
- (a) Yes. This was the case in *United States v. Kahn*—U.S.—, 14 Cr.L. 3101 (1974), where judge Campbell entered an order approving the application for electronic surveillance. The authorization order further provided that status reports were to be filed with Judge Campbell on the fifth and tenth days following the date of the order, showing what progress had been made toward achievement of the order's objective, and describing any need for further interceptions.

(b) Progress reports should be required to safeguard the Fourth Amendment guarantee against arbitrary invasions by government officials of an individual's privacy and security.

(c) Some sort of emergency provision must be set forth. By way of analogy, automobile searches conducted without the benefit of a warrant are legal under limited circumstances.

- (7)
- What is an "adequate period" of surveillance depends on the facts of each particular case. A case-by-case determination by the judicial officer involved is a far better idea than a fixed, rigid rule.

- (8)
- 18 U.S.C. Section 2516 is sufficient.

- (9)
- No. Because there is no legal distinction between "wiretapping a telephone" and "bugging a premise". The basic purpose of the Fourth Amendment is to safeguard the privacy and security of individuals against arbitrary invasions by government officials.

- (10)
- (a) Privacy is "best protected" by storage under seal forever. But there are other considerations that outweigh an individual's right of privacy.

(b) Yes.

(c) Yes.

- (11)
- 18 U.S.C. Section 2519 requires that the judge who issues or denies an interception order to report his action and certain information about the application, including the "identity of the person authorizing the application" within 30 days, to the Administrative Office of the United States Courts. Section 2519 (1)(f). An annual report of the authorizing officials designated in Section 2516 must also be filed with that body, and is to contain the same information with respect to each application made as is required of the issuing or denying judge. Section 2519 (2)(a). Finally, a summary of the information filed by the judges acting and the prosecutors approving their submissions is to be filed with Congress in April of each year by the Administrative Office. Section 2519(3).

The purpose of these reports is to form the basis of public evaluation "of the operation of Title III and to assure the community that the system of court-ordered electronic surveillance . . . is properly administered." S.Rep. No. 1097, 90th Cong, 2d Sess., 107. Adherence to the reporting requirements of Sections 2518(1)(a) and (4)(d) can simplify the assurances that those who Title III makes responsible for determining when and how wiretapping and electronic surveillance should be conducted have fulfilled their roles in each case.

- (12)
- I would think the FBI would be in the best position to answer this question.

- (13)
- (a) No.
 - (b) No.

(c) No.

STATE OF MINNESOTA
OFFICE OF THE ATTORNEY GENERAL
ST. PAUL 55155

WARREN SPANNAUS
ATTORNEY GENERAL

TELEPHONE
(612) 296-6196

August 14, 1975

Commission Counsel Milton Stein
National Commission for the Review of Federal & State Laws
Relating to Wiretapping and Electronic Surveillance
1875 Connecticut Avenue, N.W.
Washington, D.C. 20009

Dear Mr. Stein:

Below please find our response to your questionnaire on Electronic Surveillance Critics. We apologize for not returning it earlier.

No. 1-Assistant Attorney General in charge of the Criminal Division. We have participated in several electronic surveillance processes in the past.

No. 2-Yes; Yes; In some circumstances.

No. 3-We believe the list should include all crimes; No; Yes.

No. 4-Absolutely not as to all questions.

No. 5-Yes; No; No.

No. 6-No; No; Yes; Yes.

No. 7-Absolutely not; 60-90 days; No; Yes.

No. 8-No; The standards set forth on the law right now are sufficient. With the court supervising so closely as they do, there are no substantial dangers.

No. 9-No; Yes.

No. 10-Yes; Yes; Yes.

No. 11-No; No; It is presently satisfactory; No; No.

No. 12-No; Yes; No; I believe the FBI would do the best job available absent a special prosecutor; No.

No. 13-No; No; No; No; I would not do so.

Very truly yours,

[Signed] Richard B. Allyn
Assistant Attorney General

Criminal Division
207 Veterans Service Building
St. Paul, Minnesota 55155
Telephone: (612) 296-6454

THE ROSCOE POUND-AMERICAN TRIAL
LAWYERS FOUNDATION

Twenty Garden Street, Cambridge, Massachusetts 02138
617/491-6424

ANNUAL CHIEF JUSTICE EARL WARREN CONFERENCE
ON ADVOCACY

Chairman, THEODORE I. KOSKOFF

Reply to: 1241 Main Street, Bridgeport, Conn. 06604
May 20, 1975

National Commission for the Review of
Federal and State Laws Relating to
Wiretapping and Electronic Surveillance
Attention: Kenneth J. Hodson, Executive Director
1875 Connecticut Avenue, N.W.
Washington, D.C. 20009

Dear Mr. Hodson:

Your letter to your Association of Trial Lawyers of America regarding the Commission's review of federal and state laws relating to wiretapping and electronic surveillance has been referred to me for reply.

The Roscoe Pound Foundation is a research arm of the Association of Trial Lawyers of America. Last year at our Annual Chief Justice Earl Warren Conference On Advocacy, we studied the problems of privacy in a free society. I am pleased to enclose for your attention a copy of the report of that conference. I specifically commend to your attention the papers on the three divisions which we studied:

1. Electronic Surveillance
2. Data Banks
3. Political Intelligence.

I also suggest to you that Professor Herman Schwartz, who did the paper on electronic surveillance, might be a good person to testify.

In general, the recommendations of the report contained in Part A represent the thinking of the great bulk of the Association of Trial Lawyers of America. As in any conference of this type, as you will see from the list of conferees contained in the report, there was some difference of opinion. Some people adopted the position that there should be no electronic surveillance for any purpose. Most people felt that there should be no bugging for any purpose as distinguished from wiretapping, but I think you will find the report answers substantially all of the material contained in your questionnaire.

I commend also to your attention the fact that if there is any wiretapping, it was the consensus of opinion that it should be done only through the Justice Department by warrant issued after a show or probable cause. This, by the way, was also the feeling about the use of informers. The opinion was that the same criteria should be used for planting an informer as are used for other types of searches.

As a purely personal comment and as a trial lawyer of almost forty years who deals in criminal cases, it has been my view that whatever little good comes from wiretapping or electronic surveillance of any kind, is, if anything, far outweighed by the destruction of society's rights of privacy.

I hope that if you have any questions about the position of the Association of Trial Lawyers of America, you will contact me further.

Very truly yours,

[Signed] Theodore I. Koskoff

Encl.

CC: Richard S. Jacobson, Director Public Affairs and Education
Robert E. Cartwright, President ATLA

The University of Toledo

2801 W. Bancroft Street
Toledo, Ohio 43606

College of Law
Criminal Law Practice Program
(419) 537-2862

May 29, 1975

General Kenneth J. Hodson, Executive Director
National Commission for the Review of
Federal and State Laws Relating to
Wiretapping and Electronic Surveillance
1875 Connecticut Avenue, N.W.
Washington, D.C. 20009

Dear General Hodson:

Thank you for inviting me to respond to your questionnaire, which I received earlier this month. As I am in the process of

revising the first draft of my book, which I hope to complete in a few weeks, I was unable to take as much time as I would have liked to respond to the questions. I have, however, attempted to be precise, while also being reasonably brief.

If you would desire, I would welcome the opportunity to testify before the Commission.

Furthermore, if at all possible, I would like to receive copies of the material developed during the hearings at the earliest possible time. Do you have a tentative schedule for printing and publication of the hearings and other material?

Once again, thanks for inviting me to respond to your questionnaire.

Very truly yours,

[Signed] James G. Carr
Associate Professor & Director,
Criminal Law Practice Program

Enclosure

1. I am an associate professor of law at the University of Toledo where for the past five years I have directed the law school's prosecutor intern program. My experience with electronic surveillance legislation is primarily academic, as I have not directly participated in cases involving electronic eavesdropping. For the past fifteen months, however, I have devoted substantial time to research on Title III, predecessor proposals and legislation and related state statutes and cases.

2. Electronic surveillance is useful as an investigatory device, but I do not consider utility to be synonymous with necessity. In some instances, however, electronic surveillance may also be necessary. But the definition of those instances is not solely based upon the nature of the criminal activity. The feasibility of alternative methods is also an element in the definition of necessity. But unfeasibility is not synonymous with impossibility. With reference to the use of eavesdropping to control organized criminal activities and conspiracies, strategic intelligence eavesdropping appears to produce results of questionable utility, despite the claims of Title III's proponents. The clearest indication of the relative uselessness of open-ended eavesdropping appears in Assistant Attorney General Wilson's letter of Sept. 9, 1970, to Representative Celler in support of 18 U.S.C. §3504, reprinted at U.S. Code Cong. & Admin. News, 91st Cong. 2d Sess., at 4061-62. In that letter, the Assistant Attorney General revealed the evidentiary insignificance of the Justice Department's pre-Title III eavesdropping, by referring to the low number of cases in which surveillance had tainted evidence used to convict major crime figures.

In considering this document, it should be remembered that pre-Title III surveillance in any individual case was far more extensive, intense and comprehensive than the eavesdropping allowed under Title III with its probable cause, durational and minimization requirements. If, as Wilson's letter indicates, information learned in such circumstances was frequently cumulative and redundant, and often grew stale rather quickly, it is difficult to accept the indispensability of the more restricted eavesdropping allowed under Title III in enforcement activities against organized crimes and conspiracies.

Strategic intelligence gathering, surveillance in search of a suspect, appears impossible to justify under the Fourth Amendment. No effort designed to go from known criminals to their unknown crimes can meet probable cause requirements. Thus, Title III, with the probable cause and particularization requirements of §2518(1)(b) appears to prohibit strategic intelligence surveillance. See *United States v. Tortorello*, 480 F.2d 764, 779 (2d Cir. 1973). (dictum).

When used for a short period to obtain a particular conversation or discussion for its evidentiary value (rather than general investigative use), eavesdropping may be necessary to obtain such evidence. In many instances, however, consent surveillance can and will be used. It appears to me that the proponents of

eavesdropping have come considerably closer to establishing a threshold case of need and constitutionality where they state their objective as the acquisition of a specific verbal utterance, or short sequence of utterances, for evidentiary purposes. Cf. *Katz v. United States*, 389 U.S. 347 (1967).

3. The list of crimes for which eavesdropping may be used is but one of several points at which pressure may be applied or relaxed to stem or release the flow of electronic surveillance. Other pressure points include the designation of which officials may apply for and which judges may issue surveillance orders.

If legislative pressure is not applied at these points, it is necessary to impose extremely rigorous procedural controls to avoid excessive use of eavesdropping which is unjustified by either utility or need. With Title III, the pressure has not been applied at the outset to restrict the instances in which surveillance may be used. More significantly, §2516(2), which allows states to authorize the use of eavesdropping for practically any felony, provides excessive authority to the states to use eavesdropping in all major criminal investigations.

4. In theory, I support the principle that consent surveillance, where consent is induced or prompted by, or used in conjunction with law enforcement personnel, should require a prior court order. Where a party himself records the conversation, *sua sponte*, or invites a third person to listen, no legal impediments should be imposed if the private consent interception is otherwise lawful and for a lawful purpose.

I recognize practical problems involved with a court order requirement, and that there may be instances of emergency requiring immediate interception. In such cases, and perhaps in all cases, a post-interception reporting requirement might be an adequate control. If the requirement were disregarded, use and disclosure of the surveillance evidence would be prohibited, including admission in evidence.

5. If the purpose of legalized eavesdropping is investigation of organized criminal activities, it does not appear necessary to permit eavesdropping by state officers. In view of the interstate and not infrequently international character of organized crime, state officials, even with extensive surveillance authority, are not likely to achieve large scale success in dealing with a network which has only a few strands in each local jurisdiction.

The concept of centralization of decision making, and accountability in the federal system should be required of the states. County prosecutors are presently free to develop divergent standards, and extension of authorization activity to them has diffused control. Thereby, pressure has been relaxed at a second point, with the result that excessive electronic surveillance can occur at the local level without reference to the concept of centralization, which has been deemed essential by most proponents of legalized eavesdropping since 1961.

Under the present system, the danger exists that the federal process can be bypassed by recourse to a state prosecutor, who is unencumbered by the Justice Department's elaborate review procedures. The large number of federal prosecutions, particularly for gambling violations, in which state surveillance orders were obtained suggests that such bypassing is occurring. By first allowing state surveillance orders, and then failing to impose preapplication controls on state officials, Title III's two tier system invites federal officials to step down to the state courts whenever convenient. By acting through a local prosecutor, the federal authorities avoid §2516(1), and they probably have a greater range of designated offenses for which orders may be sought. Furthermore, a state applicant will have greater opportunities for judge-shopping, whereas federal applications presented to district judges may receive closer scrutiny from a judge who may not be burdened by as large a docket, who has research personnel and resources more available and who may be more responsive to Fourth Amendment policies.

6. A third pressure point in a scheme of control over electronic surveillance is the judge who can issue surveillance or-

ders. But, as indicated in Answer 5 above, Title III has no protection against judge-shopping. The effects of this practice are even more substantial than with conventional searches, because of the greater number of crucial, but discretionary and non-reviewable decisions made when a surveillance order is issued. These include the decision that investigatory alternatives are inadequate under §2518(3)(c), the period of time for which surveillance may be allowed under §2518(4)(e), whether reports under §2518(6) shall be required and who shall receive notice under §2518(8)(d) that he was overheard, though not named in the order.

The greater the number of judges authorized to issue surveillance orders, the easier and more likely it will be to present applications to favorably disposed and permissive judges. This practice abrogates the fundamental principle of detached, neutral judicial review, without which there is no protection from excessive eavesdropping.

Furthermore, continuing judicial supervision is a major, if not the only protection against the unregulated exercise by the law enforcement officer of discretion over the continuation and extent of interception. Where a failure to minimize is not corrected *in medias res* by a detailed judicial restatement of the minimization requirement as applied to the facts of the particular case, the failure to minimize will be undetected and undeterred until after the overly extensive electronic search has occurred. At that time, suppression is unlikely, and in any event *post facto* judicial intervention cannot restore conversational privacy.

Thus, I consider progress reports to the issuing judge to be essential if the concept of judicial review is to be applied to electronic surveillance. No similar requirement is present with conventional searches, to be sure. But no conventional search continues for more than a brief period of time, and its object is always a tangible, extant physical item, easily described. In such cases the problem of satisfying the particularization requirement of the Fourth Amendment arises with the description of where the item is, not what it is.

The opposite is true with eavesdropping. The description of where a conversation will occur is easy, as that is where the tap or bug will be placed. But a comprehensive and accurate prediction of a future, intangible conversation is impossible in nearly every case. If the general description of the type of conversation under §2518(1)(b) and (4)(c) is to be upheld as constitutionally satisfactory, a duty is imposed upon the issuing judge to ascertain during the surveillance whether he and the executing officer coincide in their interpretation of that description. This requires periodic review to limit the effect of the essential vagueness about the thing to be seized.

Similarly, periodic review is essential to determine the need for continued surveillance. No similar review is necessary in conventional search cases because no conventional search lasts as long. With electronic surveillance, judicial review must not be limited to preliminary approval, but should include periodic reassessment and redefinition of the authority given to the officers conducting the electronic search.

To be effective, such review will involve substantial prosecutorial and judicial time and expense. But these factors provide no justification to abandon judicial control at the point at which it has become most crucial and essential.

6a. With reference to emergency interception under §2518(7), it is impossible to gauge the need for such authority in the absence of data about the use of this section, and any abuses which have arisen. Where it develops during the surveillance that no emergency existed, and no post-surveillance application is presented by an officer who would thereby acknowledge his own bad judgment, there is no check under Title III on randomly conducted eavesdropping. When successful, such surveillance will rarely be disapproved, despite the potential for unconstitutionally allowing searches which are validated by what they discover.

Section 2518(7) should be amended to require some form of prior judicial approval before an emergency surveillance could be conducted. Even if such approval is telephonically communicated, the process for subsequent reporting, review and approval or disapproval within a short period has been begun. If the surveillance fails, the officer cannot avoid his duty to report such failure, because his application will be expected by the judge who granted informal prior approval. If no such informal review was obtained, penal sanctions should be imposed. In the rare instance where no judge was in fact available, the emergency surveillance could possibly be authorized by a chief prosecutor, who in turn had the duty to continue to attempt to secure judicial approval as soon as possible.

7. One of the major weaknesses of Title III is the opportunity for prolonged surveillance. More precisely, no justification appears for the thirty day figure in §2518(5). If eavesdropping is limited to tactical purposes, to gather specific evidence, a substantially reduced period of interception should suffice—a matter of days with a limited number of extensions available for equally short periods.

Experience under Title III indicates that the average intercept lasts about 20 days and that extension orders have been relatively infrequent. See *Report on Applications for Orders Authorizing or Approving the Interception of Wire or Oral Communications for the Period January 1, 1974 to December 31, 1974* at III (1975). At a minimum, Title III should be amended to conform to this experience.

The question of mandatory reports to the court, discussed in Item 6 above, is related to the duration issue. If no surveillance can last more than five days, periodic reports may not be necessary or feasible, and therefore they could possibly be optional. I would prefer a substantially shortened initial period—five to seven days—and similarly limited extension periods, with a total duration of approximately a month. If this change were adopted, a related control would be required to avoid surveillance which was *de facto* continuous though *de jure* terminated. A series of one week surveillances, each purportedly against a different member of a large organization, would have the same effect as a protracted tap or bug of one participant.

Prolonged surveillance appears essential where eavesdropping is conducted for a strategic intelligence, or a general rather than a specific investigative purpose. But the dubious constitutionality of an open-ended electronic search where neither the probable cause nor particularization requirements can be met can hardly be rectified by allowing the surveillance for an extended period.

7a. Although §2518(8)(d) requires notice "within a reasonable time," the ninety day maximum period for delay under that section appears to have become a minimum period, with the courts requiring an explanation only for those delays which have continued beyond ninety days. The statute should require notice within a very short period, perhaps five or seven days after termination of interception, except as postponed upon court order. A limit on the number of such postponements should also be imposed, so that notice is never withheld for longer than thirty or possibly forty five days. In my opinion, the delayed notice provision of Title III as now written assumes that considerable delay will always be required, without directly making or supporting that assertion. The presumption should be reversed, in view of the constitutional policy against secret searches, so that notice will always be prompt, except when delayed by court order for clear cause for a statutorily fixed and limited period.

8. If the period for which eavesdropping is allowed were reduced, minimization would be less significant though still important. It might be helpful to incorporate the guidelines developed by the cases under Title III concerning patterns, short calls, supervision, spot monitoring, etc., into Title III. But I consider three other aspects more important in achieving the goal of limiting interception to those conversations, or portions of conversations, which are incriminating. First is the development and

implementation of guidelines tailored to the needs of each case. Second, related to individualized guidelines, is a mandatory reporting requirement with maximum feasible disclosure of results from the surveillance as well as efforts to minimize. Third is the relationship between minimization and the authorized purpose of the surveillance. If that purpose is strategic intelligence gathering, and if such purpose is lawful, minimization is probably impossible.

9. In general, I agree with the concept that all forms of electronic surveillance should be viewed as a unitary regulatory problem. Thus, I support retention of this scheme. There are, however, some distinctions which should be acknowledged. A bug can be more pervasive, because it overhears everything within the range. Minimization therefore becomes more significant, and guidelines concerning identity of speakers, etc., are crucial. Second, as noted in Question 9, bugging usually involves entry upon private premises. If not regulated by court order as to manner of entry and emplacement of the bug, the officers may have complete discretion to select point of entry and emplacement which will bring tangible evidence into plain view. Although the inadvertency test of *Coolidge v. New Hampshire*, 403 U.S. 443 (1971) might not be met, the better protection is to provide specific instructions in the court order. These instructions should consider the need for secrecy as well as avoidance of the opportunity for a random foray along the way.

10. I do not view or interpret the provision of §2518(8)(a) as protecting privacy. Although that may have been the draftsman's intent, it is a collateral consequence. Rather, the seal appears to shift the burden from the government to show admissibility to the defendant to show inadmissibility. This makes sense generally, although sealing should be required immediately upon completion of the tape, rather than postponed until the order expires or surveillance is terminated, as now allowed.

With reference to the protection of privacy by the sealing requirement, the rights of innocent parties or of involved parties whose nonpertinent conversations are overheard have been generally disregarded under Title III. Disclosure or nondisclosure should be at the option of the party who has been overheard but is not implicated. The same should be true for nonincriminatory conversations of persons involved in criminal activity.

Finally, if the tapes are to be destroyed earlier than ten years, it should occur only upon consent of all identifiable persons overheard, not just parties to any civil or criminal litigation. Alternatively, or in addition, earlier destruction may be possible where such persons are provided with, or have the opportunity to acquire, certified copies of their overheard conversations.

11. Among the items which should be included in the reports are specific categories for consent, national security and emergency surveillance. Telephone companies should be required to keep records of all interceptions conducted to protect company property, and to provide summaries of such activity annually to the federal government and state regulatory agencies. The original records should be available upon request of subscribers whose lines have been monitored.

The Annual Reports should also include the offenses for which persons were convicted, as well as the offenses specified in the order. This information would give some indication of whether surveillance orders are obtained for one offense with a purpose of investigating other offenses, either because no present probable cause appears or the offenses are not included in the list of crimes designated by Title III or the state statute. Reversals of convictions should be indicated, and whether a defect in the surveillance authorization, application, order or execution contributed to the reversal. Finally, some standards should be developed to give more meaning to the cost data and statement of incriminating conversations.

12. If the criminal sanctions are to be effective, they must be rigorously enforced. The FBI is probably the best agency for this

activity. Internal controls within law enforcement agencies, perhaps by a reporting requirement on the equipment and its use, should be developed. Also, conspiracy charges should be used to charge (and deter) persons whose knowing acquiescence in the illegal use of such equipment by their subordinates condones and abets such use.

13. Some interception authority is appropriate, with the main problem being avoidance of excessive, unjustified or protracted surveillance. Limitations should be developed, along with the reporting requirements mentioned in Answer 11. With reference to employer monitoring of employees, cases under Title III indicate that this activity is illegal and employees have a justifiable expectation of privacy. Because of the dangers of unregulated interception, this approach should be followed.

MR. HODSON: Secondly, Mr. Chairman, I addressed a letter to the Honorable Rowland Kirks, Director, Administrative Office of the U.S. Courts, asking for his comments with respect to the reporting requirements of 18 U.S. Code 2519. He has responded to my request. And I suggest that my letter to him, together with his reply, also be made a part of the record.

CHAIRMAN ERICKSON: Both will be made part of the record.

[The documents referred to follow.]

NATIONAL COMMISSION FOR THE REVIEW OF FEDERAL AND STATE LAWS RELATING TO WIRETAPPING AND ELECTRONIC SURVEILLANCE

1875 Connecticut Avenue, N.W.
Washington, D.C. 20009
202:382-6782
May 9, 1975

Hon. Rowland F. Kirks
Director
Administrative Office of the U.S. Courts
Supreme Court Building
1 First Street, N.E.
Washington, D.C. 20544

Dear Mr. Kirks:

As an aid to your consideration of possible improvements in the reports on applications for orders authorizing or approving the interception of wire or oral communications we would like to note some of the observations of our staff in examining sample case files during their visits to local prosecutors' offices:

Costs—The staff found wide variation in the reports of costs of electronic surveillance by the different offices. For example, the District Attorney's office in Boston, Massachusetts (Suffolk County) does not report manpower costs at all. Other offices tend to form their own rough estimates of manpower costs, without considering whether to include such special costs as judge's time, prosecutor's time, or for additional detectives needed for physical surveillance to supplement a wiretap or "bug". For purposes of obtaining comparable data, it seems that a standard definition is needed of what is to be included as costs.

Accuracy and Comprehensiveness—In examining case files, our staff has discovered some blatant inaccuracies. For example prosecutors sometimes report arrests and convictions resulting

from taps when, in fact, they were based on evidence independent of the tap. There are also some areas in which responses are necessarily subjective. For example, judging what constitutes an "incriminating" statement is difficult and can be made only by a person with complete knowledge of the case. Perhaps more objective answers would be given if prosecutors reported only the number of conversations completely intercepted, as compared to the number of conversations turned off and minimized. Similarly, it is difficult to determine the number of persons intercepted on the tap or bug; more accurate figures could be obtained by requiring a report as to the number of overheard persons actually identified. The staff also believes that it is vital to obtain reports on the range of sentences actually resulting from convictions obtained with electronic surveillance evidence; this would give us some measure of the cost of the investigation as compared to the importance of the case in terms of the sentence.

Maintenance of Records—Many prosecutors, even some who command large offices, have not maintained a filing system from which they can retrieve results of their wiretaps. Indeed, some small prosecutors' offices have reported to us that, upon change of administration, the new prosecutor is unable to work with the filing system of his predecessor, and the latter's files are simply lost to further analysis and regulation. It seems important that the Administrative Office be able to enforce its record-keeping requirements and check on the proper maintenance of electronic surveillance records in local prosecutors' offices. Thus, it might be helpful in the long run if the law required all prosecutors to keep specific information in the file of each wiretap case. We would appreciate your thoughts on this problem.

Consensual Eavesdropping—Law enforcement authorities have been almost unanimous on the need to use consensual electronic surveillance for law enforcement purposes free of court-order requirements. But there is concern over the distribution of electronic surveillance equipment without responsible supervision. A few offices keep records of consensual eavesdropping. Do you believe that reports should be required on the number of consensual surveillances performed by law enforcement authorities, even though court-orders are not required?

Enforcement of Reporting Requirements—Do you have any views of how reporting requirements can be enforced? One thought that has occurred to us is to change the law to make the Attorney General of each state responsible for records and reports of wiretaps by prosecutors in his jurisdiction.

Receipt and Compilation of Reports—What are your views with respect to whether the Administrative Office should continue to have the responsibility for receiving and compiling wiretap reports?

Computer Analysis—There are several interesting, but intricate, comparisons that could be made using data that could be required in reports to the Administrative Office. We would like your professional views on the possibility and need for computerizing the electronic surveillance data submitted to your office.

It is clear that the views of the Administrative Office on these and other matters pertaining to the electronic surveillance reports are vital to the Commission's work, and we look forward to your comments.

Sincerely,

Kenneth J. Hodson
Executive Director

ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS

Supreme Court Building
Washington, D.C. 20544

ROWLAND F. KIRKS

Director

WILLIAM E. FOLEY

Deputy Director

May 30, 1975

General Kenneth J. Hodson

Executive Director

National Commission for the Review of Federal and State Laws

Relating to Wiretapping and Electronic Surveillance

1875 Connecticut Avenue, N.W.

Washington, D.C. 20009

Dear General Hodson:

We have reviewed the observations noted in your letter of May 9, 1975 and have found many of your comments to coincide with our own. However, we do have some additional comments and suggestions with respect to the Administrative Office's involvement in wiretap reporting. These are as follows:

Costs: A standard definition of "costs" is already stated in the "Regulations Relating to Reports on Intercepted Wire or Oral Communications . . ." which is sent to prosecuting officials in November of each year. In Part II, Sec. 201 (4)(b)(v) of these regulations "costs" is defined as follows:

"'Manpower' costs should include the cost of the time spent by officers or employees both in installing and in monitoring the equipment and time spent in preparing transcripts. 'Resource' costs should include the costs of installation where the installation is done on a contractual basis; rental, lease, or amortization of equipment; and the cost of supplies including magnetic tapes and discs."

The cost of time spent by a detective on physical surveillance to supplement the wiretap should be included in manpower costs. However, we do not feel that the cost of the judge's and prosecutor's time would add significantly to the cost figures and would at best be difficult to measure.

Accuracy and Comprehensiveness: Reports on the total number of communications intercepted and the number of such communications that were turned off and minimized would be useful and objective. Reporting the approximate number of incriminating intercepts should continue since the purpose of the wiretap is to gain incriminating evidence. The subjective nature of the word "incriminating" is recognized, but we do not feel that it is so subjective as to result in inaccurate reporting.

Sentencing information could be reported and used in an interesting comparison with the cost of the wiretap. However, in order to make a sound determination of the importance of a case in terms of the sentence, it would be necessary to receive reports on the statute and penalties for each type of offense since penalties vary from state to state. Wiretap cost figures, in most cases, are only reported upon termination of the wiretap whereas convictions related to the wiretap and therefore sentences are also obtained from supplementary reports received in subsequent years.

Maintenance of Records: Under the present law the Administrative Office has no record keeping requirements as pertains to records maintained in local prosecutors' offices. Monitoring such records at the national level would be a formidable undertaking and would require additional personnel.

Since it is required by law that prosecutors report specific information regarding wiretaps, it would seem imperative that such information be kept in local prosecutor files. One suggestion is that the statute could be amended with more emphasis placed on the requirement that a wiretap report *must* be sub-

mitted and *must* be received no later than January 31 of the year following the termination of the wiretap. Further, such reports could be required of each prosecutor on wiretap activity originated and/or terminated during his time in office for each calendar year. We too have noted that many of the prosecutors leaving office do not alert incoming prosecutors to their reporting responsibilities.

Consensual Eavesdropping: Theoretically, it may be desirable to obtain reports on consensual wiretaps. Practically, it would be extremely difficult, if not impossible, for law enforcement authorities or prosecutors, especially in large cities, to report on consensual wiretapping activity. The volume of this type of wiretap would prohibit reporting.

If there is concern over the distribution of electronic surveillance devices, then perhaps stricter controls at that level should be provided.

Enforcement of Reporting Requirements: If the Attorney General of each state were responsible for the wiretap reports of the prosecutors in his jurisdiction, he might be in a position to be effective in enforcing the reporting requirements. The state Attorney General could insure that each prosecutor in his state is fully informed of the wiretap statute's reporting requirements and that the prosecutors conform to both State and Federal reporting regulations. Just by virtue of being in the same state, the Attorney General would be more likely to be cognizant of any change in prosecutors than would a federal agency in Washington, D.C.

Receipt and Compilation of Reports: Although the collection and compilation of wiretap reports is not inherent in the function of administering the federal courts, it has been assigned to us by Congress and we must, however, accept this responsibility. If the Wiretap Commission were to become a permanent agency, then there would be no question but that the wiretap reporting should be assigned to that agency.

Also as long as the reporting stays at its present level, the assignment is not unduly burdensome. If wiretap reporting should increase as proposed in H.R. 3113, an entire "wiretap" staff would have to be funded in order to handle the volume. At that point the reporting function should undoubtedly be removed from the Administrative Office. To assign such a task to this Office would be to lose sight of our primary responsibility—which is to the Federal courts.

Computer Analysis: Computerizing electronic surveillance data would be useful for data analysis. It would also be of service in preparing the report itself, especially with regard to matching prosecutor and judge reports and the preparation of the full and complete report transmitted to Congress. Precautions should be taken to safeguard unpublished wiretap information, such as current calendar year reports. Wiretap information is available to *no one* until its release to Congress in April of each year. All published reports are widely distributed by the Administrative Office and are available to anyone upon request.

If published electronic surveillance reports are to be computerized, we feel that it would be inappropriate for the Administrative Office to assume that job since our computer responsibility is to the Federal courts.

We hope you find these responses and suggestions helpful. The opportunity to express our views is certainly appreciated. If you or your staff should have further questions or observations on wiretap reporting problems and procedures, please let us know.

Sincerely yours,
[Signed] Rowland F. Kirks,
Director

CHAIRMAN ERICKSON: Judge Stern, in accordance with the rules of the Commission, will you be sworn.

[Whereupon, Judge Stern was sworn by the Chairman.]

TESTIMONY OF THE HONORABLE HERBERT J. STERN, NEWARK, NEW JERSEY

CHAIRMAN ERICKSON: We are, indeed, honored to have you here. I think most members of the Commission know of your work, both as a Federal judge and as a Federal prosecutor.

I think the Commission should be made aware, as well as the record, of your background as a highly effective investigator of corruption and of some political evils.

Your work has caused other prosecutors to model their methods of investigation after your work, and, as I understand it, you were consulted by the U. S. Attorney in Baltimore upon start of the investigation which led to the resignation of Vice President Agnew; is that correct, sir?

MR. STERN: Yes, sir, that is right.

Well, I don't know how you want to proceed, Judge. I have furnished, at the request of Mr. Hodson, a statement.

CHAIRMAN ERICKSON: A prepared statement that we will cause to be filed for the record.

[The prepared statement of Herbert J. Stern follows.]

United States District Court

District of New Jersey

CHAMBERS OF
HERBERT J. STERN
JUDGE

UNITED STATES COURT HOUSE
NEWARK, N.J. 07101

May 28, 1975

Kenneth J. Hodson
Executive Director
National Commission for the Review of Federal and State Laws
Relating to Wiretapping and Electronic Surveillance
1875 Connecticut Avenue, N.W.
Washington, D. C. 20009

Dear Mr. Hodson:

Thank you for your letter of May 22, 1975, requesting me to make a written statement concerning the application of the Federal Electronic Surveillance Law, and to give oral testimony concerning it on June 10, 1975.

As I discussed with Mr. Milton Stein of your staff, as a federal judge who must from time to time sit on cases which may involve the construction of the statute (Title 18 U.S.C. Sections 2510-2520), and for the further reason that as United States Attorney for the District of New Jersey I never had occasion to make an application for electronic surveillance pursuant to that statute, I do not think it appropriate for me to testify concerning the details of the administration or application of the statute itself.

On the other hand, I gather that your Commission is interested in the usefulness, or the lack of it, of electronic surveillance in the investigation and prosecution of cases involving political corruption and organized criminal activity. I have had, as United States Attorney, familiarity with these types of cases and I think

I can appropriately make a statement concerning the role, if any, that electronic surveillance has played in the investigation and prosecution of these matters during my tenure as United States Attorney. Accordingly, the following constitutes my written statement on this limited aspect of your subject matter.

Based upon my experience as a federal prosecutor, I am convinced that non-consensual electronic surveillance, as authorized by Title 18 U.S.C. Sections 2510-2520, is virtually useless in the investigation of cases involving political corruption, labor racketeering and organized white-collar crime. My experience as a federal prosecutor in New Jersey commenced in January of 1966, when as a trial attorney in the Organized Crime and Racketeering Section of the Criminal Division of the United States Department of Justice, I was sent to New Jersey to convene a special grand jury to probe corruption in the Operating Engineers Union, and continued until January of 1974 when I was inducted as a United States District Judge for the District of New Jersey. During that period, between January of 1966 and January of 1974, I assumed the positions of Chief Assistant United States Attorney on September 3, 1969, and United States Attorney on February 1, 1971.

During my eight-year tenure I participated in a number of grand jury investigations of cases involving political corruption, white-collar crime and labor racketeering, and also in many criminal prosecutions which were the product of these investigations.

For example, during this period a substantial number of public officials of New Jersey's largest city, Newark, including the incumbent Mayor, Corporation Counsel, Director of Public Works and several councilmen, were charged in one indictment with conspiring to receive and with actually receiving payments extorted from businessmen who sought to do business within the City of Newark, and all who went to trial were subsequently convicted.

Similarly, in Jersey City, New Jersey's second-largest city, the incumbent Mayor, President of the City Council, Business Administrator and numerous other public officials were charged in one indictment with similar activities and subsequently convicted.

In Woodbridge, New Jersey's sixth-largest community, the incumbent Mayor and President of the City Council were charged with and subsequently convicted of receiving \$110,000 in bribes from the Colonial Pipeline Co. of Atlanta, Georgia.

In Atlantic City, another major New Jersey community, the incumbent Mayor and the incumbent Director of Public Works, as well as many other city and county officials were charged in one indictment with similar activities and subsequently convicted.

In addition to these investigations and prosecutions of corrupt municipal governments, the United States Attorney's Office brought numerous cases against individual federal, state, county and municipal office holders who had committed corrupt acts either for their personal enrichment, or for the enrichment of their particular political party. For example, two successive Secretaries of State, Robert Burkhardt (Democrat) and Paul Sherwin (Republican), and two successive State Treasurers, John Kervick (Democrat) and Joseph M. McCrane, Jr. (Republican), were indicted and ultimately convicted, as were Nelson Gross (former Republican State Chairman and Special Assistant to the Secretary of State of the United States, in charge of the American drug program abroad), and Cornelius Gallagher (Democrat), seven-term United States Congressman.

In addition, the office of the United States Attorney for the District of New Jersey handled many other such cases while I was associated with it.

I am thoroughly familiar with each of the prosecutions mentioned above, as well as with many other investigations and prosecutions of corruption in government, the trade union movement and the business world which were conducted by the United States Attorney's Office between September of 1969 and

January of 1974. Based on personal knowledge, therefore, I can unequivocally state that no wiretap or non-consensual eavesdropping device was ever employed in connection with the investigation of any of these cases. Moreover, I can unequivocally state that such investigative tools would have been virtually useless to us in the investigation of these matters, and it is for that reason that not even one application for an electronic surveillance order was ever made in respect to any of these investigations.

The preceding constitutes my written statement. I would like it clearly understood that my statement does not cover investigations into unlawful gambling activities or into narcotics activities. These investigations were primarily handled by the Organized Crime and Racketeering Section's Strike Force in the District of New Jersey and not by the United States Attorney's Office. I therefore have no first-hand information concerning the effectiveness of electronic surveillance as an investigative tool in those types of cases and, while I may well have an opinion on that subject, I do not presume to offer it with the kind of expertise and familiarity with which I believe I can speak in the area of organized political corruption and organized white-collar criminal activity.

I hope this meets the request which you made in your letter. I understand that I will be testifying on the afternoon of June 10, 1975. I await your further advice and instructions on this matter.

Sincerely,

[Signed] Herbert J. Stern
United States District Judge

CHAIRMAN ERICKSON: If you'd like to make a brief summary of that, we'd be delighted to hear that.

MR. STERN: Has each member been furnished a copy?

CHAIRMAN ERICKSON: Every member has been furnished a copy.

MR. STERN: Then I think I won't bore them by resaying what they have already seen.

I will be available to take any questions, sir, with respect to anything that I have put into my prepared statement.

CHAIRMAN ERICKSON: As I understand it, you have conducted a number of major investigations, and in doing that you did not feel that you needed to use nonconsensual electronic surveillance.

MR. STERN: That's a fact. In not a single one of the investigations in which I participated and, indeed, in not one investigation at all conducted during my tenure in office was there an application made for an electronic surveillance order, nor did we feel that there was any necessity for such an application.

Indeed, in terms of the cases which I listed in my prepared statement, there was not even one consensual electronic device utilized, although in some other ones, a very small number of other ones which were not listed because they were rather minor cases compared to the ones that were mentioned, there were in one or two instances consen-

sual recordings made by one participant in the conversation.

CHAIRMAN ERICKSON: I might ask this: In your work as a prosecutor—and you have had about as much experience in this field as any that I know of—did you feel that it was necessary to look to this act to complete your investigation, the Omnibus Crime Control and Safe Streets Act, Title III thereof?

MR. STERN: Well, I can give you my objective evaluation, which is no. And the best objective evidence that I can offer is that not only did we not consider it necessary but, because we didn't consider it necessary, we never attempted to utilize it. Indeed, to be very frank, it would have been very difficult in my estimation to know where to begin, for the kind of crimes we were investigating were not those in which the telephone plays an important role as an instrumentality of the crime itself.

Kickbacks on contracts, payoffs to politicians, are not, in my experience, at least—or were not in my experience—practiced by such people on the kind of revolving-door basis which required the continuous use of the telephone for the commission of the crime itself.

And the cases that we made in New Jersey, and based on my consultations with George Beall, United States Attorney for the District of Maryland, I think I can safely say the cases he made in the State of Maryland were developed from books and records and information developed from them by accountants in which the major effort was a search for illicit pools of cash.

That is a rather lengthy answer to a short question, but I think it summarizes the facts.

CHAIRMAN ERICKSON: Of course, there are certain crimes that fall within the jurisdiction of the United States Attorney where the telephone is part and parcel of the crime?

MR. STERN: That is right.

CHAIRMAN ERICKSON: In those cases, do you feel that it is the *Rathbun* exception that is built into the Title III provisions that avoids the need for any court-ordered electronic surveillance?

MR. STERN: No, rather the unique experiment that was conducted during my tenure as U. S. Attorney by the Department of Justice where, as you know, Judge, what they called Task Forces or Strike Forces were sent into regions of the country, primarily charged with the obligation of investigating gambling-type offenses. Since it was largely their function to conduct those types of investigations, they did employ nonconsensual electronic surveillance techniques pursuant to court order.

So I don't want to imply that in my jurisdiction during my tenure there were never such applica-

tions made by a Federal investigative agency, but rather that it was not done by my office simply because my office did not have any real—

CHAIRMAN ERICKSON: You didn't get into the gambling area?

MR. STERN: Exactly.

CHAIRMAN ERICKSON: Or into some of the areas that would be within the jurisdiction of the Organized Crime Task Force?

MR. STERN: That is exactly right. Under the guidelines established by then Attorney General Mitchell, there was an attempt made to delineate the primarily investigative responsibilities of the Strike Forces in the area, on the one hand, and the United States Attorneys on the other. And this was primarily their responsibility. Indeed, such information as the Federal Bureau of Investigation or other agencies had concerning those kinds of activities were, pursuant to those guidelines, to be referred initially to the Task Force's personnel. So we did not employ such devices in such investigations, precisely because ours was not the primary focal point of the investigations of those kinds of crimes.

And I do not mean to imply by the statement that I have submitted that in the investigation of gambling offenses electronic and consensual electronic surveillance is not a useful device. I don't mean to imply that at all, but rather to give you the benefit of my primary experience which is in another area of investigation.

CHAIRMAN ERICKSON: The area of investigation you are directing your remarks to would be limited to what four corners?

MR. STERN: Well, I think part of the problem in dealing with the subject is the lack of precise definitions. No one to my knowledge has been able to define to my satisfaction precisely what we mean when we refer to "organized crime." So it is very difficult, you see, because, unlike the field of certain sciences, there aren't precise definitions. I am referring to political corruption issues.

When someone on the street corner takes a hundred dollars from a bookmaker, I don't regard it as a political corruption case. I regard it as graft, but this is not what I mean by a political corruption case.

Nor, in any lists that I would ever compile, if I were to do so, of the public officials prosecuted by our office, would I ever include local policemen on the corner who take such kinds of graft. We'd prosecute them but we wouldn't list them in that kind of way.

I don't know if I am making any sense.

CHAIRMAN ERICKSON: I think that is an excellent start.

MR. STERN: So when I speak of mythical corruption cases, I am talking about the public official, elected or appointed to the public office in any one of the three branches of government, who would take money for his own personal enrichment or for the enrichment of his party or for the enrichment of some third person, and in return, therefore, grant or deny some governmental favor.

CHAIRMAN ERICKSON: And you feel that to make that type of investigation you don't need the electronic surveillance investigating techniques that are outlined in the statute?

MR. STERN: Absolutely, I feel that way. It has been my experience that it was not useful.

I know, for example, in the recent report filed by the Administrative Office of the U. S. Courts which lists the total number of applications for electronic surveillance orders made by the states, on the one hand, and the United States on the other, and provides a breakdown of kinds of crimes being investigated, in the whole country there are only 25 applications under the title of "bribery." Of those, none were made, apparently, by the United States Attorneys or United States agents. And finally, of the remaining 25, which were obviously state applications, I would suspect a number had to do with illicit payments between local police officials and gamblers, which is not the kind of thing I'm talking about.

CHAIRMAN ERICKSON: In connection with the kind of work you did as United States Attorney, you, of course, had occasion to become familiar with *Berger v. New York*, and the experience that the State of New York had in passing upon Section 813(a) of their state statute which permitted electronic surveillance. And in that particular case, you recall, there was a question of whether liquor licenses were being bought and sold in the New York area. And from the history that has been laid out in the Standard of Criminal Justice on electronic surveillance, that was very capably delineated by Professor Blakey who is on our Commission, it becomes quite apparent that when the State of New York looked to electronic surveillance there was no other means of breaking up this political corruption that was tied to buying and selling liquor licenses.

MR. STERN: Well, I worked in District Attorney Hogan's office at the time of the SLA (State Liquor Authority) investigation which led ultimately to the conviction of the former Republican state chairman of the State of New York, and I think Mr. Bernstein was the name of the chairman of the SLA. I have a feeling he was ultimately convicted as well, but I may be incorrect.

And I would yield to the expertise of others in the area, but I am not wholly persuaded that electronic surveillance resulted in the success of that investigation. And moreover, I would respectfully point out that those kinds of investigations have been going on in New York, at least in my limited research, for so many years, I begin—if you will grant me a moment's indulgence—I begin with the Tweed days of 1871. The kind of graft and corruption experienced in the days of William Marcy Tweed is exactly the kind of corruption I'm talking about—kickbacks.

In that instance, if I remember correctly, it focused on the building of a courthouse that probably cost more than any other building in the United States.

Boss Tweed was brought down not by any electronic surveillance. Indeed, obviously, there weren't telephones then. He was brought down because of the books and records examination ultimately made by Samuel Tilden acting in concert with a publicity campaign of the *New York Times* of that time and Thomas Nast, the cartoonist.

That kind of corruption, which was probably the most pervasive the country has seen, strangling an entire city, the major city of the United States at that time, was brought down and the chief perpetrator convicted without the necessity of using electronic surveillance.

I move along to 1894 and the Lexow Commission which investigated corruption in the City of New York. As you no doubt know, it was sparked by the campaign of Charles Parkhurst who demanded the New York Legislature investigate the tie-in between gambling, prostitution, corruption, and the New York Police Department.

That Commission in 1894, so ably reported by Lincoln Steffens in his work, revealed a large amount of wrongdoing by policemen. As a matter of fact, the entire political structure of New York was changed for awhile because graft was out and reform was in as a result of the Committee's investigations.

But those were done without the necessity of electronic surveillance.

As far as I can tell, neither did William Travers Jerome employ electronic surveillance.

If we move along to the period when Jerome was District Attorney investigating graft, corruption, and particularly gambling in New York, he wound up putting in jail the chief New York gambler, a man by the name of Richard Canfield, without, to the best of my knowledge and belief, using any electronic surveillance.

And to bring us up to date rather rapidly, in the days of Samuel Seabury in which that remarkable

man served on three separate appointments, one by the Appellate Division of the State of New York, another the Hofstadter Committee to investigate Mayor James Walker, and finally as an investigator appointed by Governor Franklin Delano Roosevelt to see whether or not District Attorney Crane would be replaced, in all three capacities he achieved remarkable and noteworthy success in rooting out corruption, to the point where the Mayor of New York had to resign and sail over to Europe in disgrace, and I am unaware of any electronic surveillance he found it necessary to employ in any of those investigations either.

So I think there is ample precedent for what I say, not only in what we have done in New Jersey, but in what others have done in meeting this situation elsewhere.

CHAIRMAN ERICKSON: As I understand it, you are limiting the area that you say falls within the scope of not requiring electronic surveillance to the political corruption area?

MR. STERN: That is correct.

CHAIRMAN ERICKSON: You are not going into gambling?

MR. STERN: I am not saying that it is not a useful device in gambling.

CHAIRMAN ERICKSON: Or necessary?

MR. STERN: Or even necessary.

CHAIRMAN ERICKSON: And the same would be true on the narcotics side, as I understand?

MR. STERN: That is correct.

CHAIRMAN ERICKSON: Or on organized crime, if we were able to reach a definition on that.

MR. STERN: If you were able to reach a definition, I'd be able to confront the question, but it's awfully difficult for me, Judge, to deal with a creature who nobody seems to be able to put four sides on.

CHAIRMAN ERICKSON: I can understand that. One further question going to this whole area:

When it comes to electronic surveillance, as you know, Title III put an invitation in to the various states to enact legislation of their own patterned after the Omnibus Crime Control and Safe Streets Act.

In the State of New Jersey they did enact legislation, as I understand it.

MR. STERN: Yes.

CHAIRMAN ERICKSON: It had a five-year limitation; is that correct?

MR. STERN: Yes. According to the newspaper accounts that I have read, the New Jersey Legislature has just amended the law. But, of course, I have no first-hand knowledge of that anymore.

CHAIRMAN ERICKSON: I see.

Did you cooperate with the New Jersey law enforcement officials during the period that you were in the United States Attorney's office?

MR. STERN: I don't know if you realize it, but it is a very difficult question to ask me to answer.

CHAIRMAN ERICKSON: I do.

MR. STERN: As long as you understand that the parameters may be rather broad, I will try to answer it.

On certain levels there was good cooperation; on certain levels there was very bad cooperation.

When certain investigations were conducted by my office and touched highly placed personages then in the Governor's Cabinet, there was a remarkable lack of cooperation.

I don't think anybody would be especially surprised about that. There is no one of us so fine a human being that we can be safely entrusted with the investigations of our friends and colleagues.

I claim no great superiority in this area, but when such investigations conducted by my office touched those areas there was not cooperation.

CHAIRMAN ERICKSON: This is in the local corruption area?

MR. STERN: Yes.

CHAIRMAN ERICKSON: That was the purpose of the question because it is obvious that you couldn't cooperate in that area.

MR. STERN: Well, it seems to me that, first of all, maybe we could, but we soon learned in some cases we couldn't.

It is easy for a Federal law enforcement officer and state law enforcement officer to cooperate on a bookie or petty thief. It is quite another thing when you are talking about a secretary of state or state treasurer or the likes of that. Then one finds that self-interest may dictate a lack of cooperation.

So I'm sorry for the length of the reply, but as you see, it is a rather broad area.

CHAIRMAN ERICKSON: It was meant to be broad and it was the answer I hoped we would be able to get for the record.

Professor Blakey.

MR. BLAKEY: Judge, I wonder if you'd comment on the historical analysis that you made of Jerome and some of the others.

Was there a suppression rule in New York at that time?

MR. STERN: The suppression rule, Professor, wasn't passed until 1914 by the United States Supreme Court in the *Weeks* case, *U.S. v. Weeks*, and it was not made applicable to the states until the *Mapp* case in 1961.

MR. BLAKEY: Consequently, there were no practical limitations on those prosecutors. Those rules that existed then weren't enforced in the courts by the suppression sanction?

MR. STERN: You mean by way of search and seizure?

MR. BLAKEY: Yes.

MR. STERN: I suppose that is true.

MR. BLAKEY: Are you familiar with the techniques they used in making those investigations?

MR. STERN: I am familiar in some respects.

MR. BLAKEY: Take Jerome's prosecution of Canfield, for example.

MR. STERN: Yes. If my memory serves me, in Richard O'Connor's book, *The Courtroom Warrior*, which you may be familiar with, he details a history of long attempts by Jerome to bring Canfield, who was—

MR. BLAKEY: —responsible for much of the gambling at Saratoga.

MR. STERN: Right.

I think ultimately they did not get Canfield on the basis of any search and seizure which would be called unlawful or unconstitutional today.

MR. BLAKEY: Were there raids without search warrants on his casino?

MR. STERN: There were raids with search warrants on his casino as well, and ultimately Jerome made the case against Canfield, if my memory serves me, by obtaining the testimony of certain prominent New Yorkers who had gambled in his establishment against him. And if I recollect correctly, Canfield pled guilty.

If that is wrong, please refresh me.

MR. BLAKEY: It is my recollection that some search warrants were used in some of the situations, but if we apply any Fourth Amendment test of probable cause or particularity, they'd probably flunk. They'd certainly flunk the Spinelli test.

MR. STERN: They might, but if Mr. Jerome worried about Spinelli, it may have been he could have presented the magistrate evidence which would have satisfied the magistrate. I think it's unfair to judge his affidavits on court rules passed 40 or 50 or 60 years after his time, because he didn't have those in mind when he brought the affidavit in court. It seems to me the mere fact he did go by affidavit and warrants is some indication that he wasn't really—

MR. BLAKEY: He was also dealing with what could be fairly described as open gambling. This was not bookmaking over phones. It was an open casino in downtown Manhattan. Anybody could have walked into it.

MR. STERN: Not anybody.

MR. BLAKEY: Relatively speaking, it was wide-open gambling.

MR. STERN: A policeman couldn't walk in there. Mr. Jerome couldn't walk in there. I suspect

if you and I had been living in that community we couldn't have walked in there.

You are probably more expert than I am, but one wonders how secret any widespread gambling operation is when, by definition, they have to have a lot of customers.

MR. BLAKEY: I am trying to bring out that the rules of search and seizure in dealing with gambling then were somewhat different than they are today.

MR. STERN: I think that is right.

MR. BLAKEY: Is there any indication that Canfield used violence to enforce his rules?

MR. STERN: We know this. In 1912 Herman Rosenthal was shot dead on a street corner of New York by Whitey Lewis and Dago Frank and Gyp the Blood—those were the names employed at the time. And ultimately in the prosecution, the District Attorney proved that Lieutenant Charles Becker of the New York City Police Department ordered that execution and ultimately became the first police officer ever electrocuted in the electric chair.

That sounds to me like a pretty serious kind of problem. That's 1912.

MR. BLAKEY: Moving up a little bit in time, I take it you are familiar with the work of Frank Hogan's office?

MR. STERN: I had the distinct honor of serving there.

MR. BLAKEY: Are you generally familiar with the liquor investigation?

MR. STERN: I wasn't in his Rackets Bureau. I was in the Homicide Bureau. I am only generally aware of the SLA investigation—are you referring to it?

MR. BLAKEY: That is right. Based on your general knowledge, do you think that case could have been made without electronic surveillance, both the consensuals in the early stages and ultimately the bugs that implicated Mr. Morehouse and Judge Osterman?

MR. STERN: Mr. Blakey, I find in life you come to a fork in the road where you must take one path or another. Having taken one path, it is awfully difficult to cast one's mind back and speculate what would happen if you had taken the other path.

I submit to you that it would be almost impossible for anybody to say with any degree of assurance what would have happened if other investigative techniques had been employed.

I am prepared to accept the fact if you tell me so because I have no personal knowledge that wire-tapping or electronic surveillance played an important role in that investigation. I would be very reluctant to accept the hypothesis, which could only be a hypothesis, that if those techniques were not employed the cases would not have been made.

I happen to believe that Frank Hogan and the dedicated men of his staff had enough ingenuity and ability so if this technique had been denied them, as it was denied to men like Jerome, and not available to men like Seabury, they might have made the cases anyway.

MR. BLAKEY: Moving on to another matter, which I suspect is more vital, I wonder if you would discuss, as both a former Federal prosecutor and a Federal judge, what you understand to be the constitutional role of a Federal judge sitting to supervise various law enforcement techniques and also the practical realities of it.

Let's see if I can't pose the broad problem this way.

We read endlessly in Supreme Court cases that the independent magistrate must be interposed between the citizen and the policeman. And certainly as a matter of constitutional theory, this is a very attractive ideal.

And yet, we turn to study after study—I am referring now particularly to the American Bar Association studies—that indicate in most search warrant applications that the judge is little more than a rubber stamp.

In the annual reports on the wiretap act, except for one Federal judge in Nevada and two or three judges in Connecticut, no judge has ever denied—on the Federal or state level—with those exceptions—an application for wiretapping.

It is my understanding that prosecutors are serving as the screening level, and they are being denied at that level, and that doesn't show up in the reports.

I am really trying to get you to share with us your notion of not only what it ought to be in light of the Supreme Court's statements, but, as a practical matter, how much can we expect from the judiciary, day to day, acting as a sergeant in the police department, telling the police to do this and not do that.

MR. STERN: Well, it is one thing—I think I have the question in my mind, although it certainly is a strike between the knees and shoulders, and one can swing and hit it from almost any direction.

It seems to me it is one thing for a judge to say to a prosecutor, "You can't do something," and it's another thing to suggest to him affirmatively what to do.

Do you want me to get into that area?

MR. BLAKEY: No. I take it the role would normally be negative, "You may not do this."

MR. STERN: Yes. Before the search or eavesdropping occurs, or after it occurs, the function is basically the same. I suppose it should be argued in the latter event, however, when it is done without

prior approval, at least the invasion of privacy occurs before the judge ever gets to look at it, and it might be better in the sense of the area of privacy, since even the sharpest critics of the judicial advisory role would not deny to the judge the function of reviewing it afterwards.

Is that right, Professor?

MR. BLAKEY: In fact, the studies indicate that the post-search review, which is on a written record, with counsel present, and in the context of a courtroom proceeding is effective. In some cases, you have the unusual situation occur where the judge who issued the application turned around, after counsel was present and he had an opportunity to reflect, and he suppressed his own wiretap.

MR. STERN: Yes.

MR. BLAKEY: I am not limiting this entirely to wiretap. I am talking about search and seizure issues generally.

MR. STERN: I have one problem, Professor. I have presently before me a case on habeas corpus in which such issues are raised.

MR. BLAKEY: Can you just talk about it on a philosophical level?

MR. STERN: Well, it is the *People v. Petillo*, in which the Supreme Court of New Jersey has made certain findings in that area which are being challenged before me.

Do you understand what I mean, Professor?

MR. BLAKEY: Yes.

MR. STERN: And I have no intent of depriving you of any useful information. Once that case is decided, if ever you wish to have me back again, I'd be delighted.

MR. BLAKEY: Just for the record, if I ever get to talk to another Federal judge, the kinds of questions I would have liked to have asked you are, "All right; wiretaps, but why consensuals?"

MR. STERN: Why consensuals?

MR. BLAKEY: Why should consensuals be subject to a warrant?

MR. STERN: That is not what you asked me a moment ago.

MR. BLAKEY: It is clear in the statute that warrants are required for wiretapping and bugging, and it is clear from the Supreme Court cases that this is required. So really we have no options there.

But the proposition is being advanced—and I think with some credibility and some forcefulness—that the warrant processes that are constitutionally required as to wiretapping should be statutorily extended to consensuals, where there is now no constitutional requirement for a warrant.

MR. STERN: The *White* case.

MR. BLAKEY: This is the one-party consent case?

MR. STERN: The *White* case, the *Lopez* case; yes.

MR. BLAKEY: Before we take that jump and extend these roles elsewhere, it seems to me we should ask how does it work in its present function, and if we could meaningfully expect it to work as well in the other area. And I wanted you to share with us whether you think the judge could perform a meaningful role in enforcing a court-ordered system on one-party consent electronic surveillance.

Can you answer that?

MR. STERN: Yes, I can try to answer that. That is essentially a different question than the one you were asking.

As far as I am aware, the United States Supreme Court has made clear, although in a sharply divided opinion, that the area of consensual electronic surveillance is simply not, under our Constitution, to be concerned about, the theory being if A speaks to B, A takes the chance that B is going to repeat verbatim, if he has that kind of memory, what A has said, or make a reporting or otherwise record it.

Indeed, it may be that if he is going to give you an account at all of what is said, the very best account would be the actual words A has used. Because B, if speaking out of recollection, may be wrong or lying or a number of things. But if B has an actual recording of what A has said, no one can challenge the accuracy unless there are technical problems.

That being the law, I don't know what function the judge would perform either before a consensual recording was made, or after it was made, unless you wanted to post into the law a requirement of probable cause for consensual recordings, the kind such as there is in a nonconsensual area.

Is that what you mean?

MR. BLAKEY: Yes.

MR. STERN: If that is what you propose, then I suppose the judge has the same function in determining probable cause for consensual electronic recording as he does for nonconsensual, to determine whether or not there is probable cause.

MR. BLAKEY: Do you think it would make sense from a policy point of view—not from a law enforcement point of view—to put those kinds of restrictions on consensu-als and involve the judiciary in them?

MR. STERN: I don't think the question of involvement of the judiciary is a relevant one, as I am trying to indicate. It doesn't matter, in my opinion. The real question you are asking, I think, is whether or not you ought to make a requirement of probable cause, in other words, build probable cause into the requirement for a consensual recording. That is

a policy issue. Once you decide that issue, you leave the judiciary no alternative because sooner or later the judiciary will have to review whether or not there was probable cause.

MR. BLAKEY: Do you think it makes a difference whether the review was prior?

MR. STERN: It makes a difference only to the extent that if it is prior, as well as subsequent, you at least offer the potentiality that some potential breach of privacy will not occur, rather than limiting it to redress after it has, in fact, occurred. That is assuming, of course, that you have defined by due legislation that consensual recordings are breaches of privacy.

On the privacy question, I don't think, in my opinion, that if B records what A is saying to him, B is violating A's privacy. But I can well realize other people may disagree with that.

In any event, I am not saying that as a judge but as an individual.

Does that answer your question?

MR. BLAKEY: Yes, thank you.

I have no further questions.

CHAIRMAN ERICKSON: Does that complete your questioning, Professor Blakey?

MR. BLAKEY: Yes.

CHAIRMAN ERICKSON: Professor Remington.

MR. REMINGTON: Judge, I just have one or two questions.

I am not sure whether we have a conflict between some prior testimony which we heard yesterday and your testimony today with regard to one question that this Commission is concerned with, and that is the effectiveness of electronic surveillance.

And I take it that most of your testimony was addressed to that question with respect to official corruption cases.

MR. STERN: Yes.

MR. REMINGTON: My recollection of the testimony yesterday and on previous occasions was that it is very important to have the right to have a consensual overhear, as it was described, in cases of official corruption because very often it is a one-on-one situation, in bribery cases in particular, and it is important to have more than the word of the informant or, in his own defense, the official.

Do you disagree with that? That is, do you disagree with the assertion that it is extremely important to have the right to record, with the consent of one party, conversations involving, for example, the bribery of a public official?

MR. STERN: It is most difficult to deal with your question in terms of absolutes. I mean no offense to the question, but, "Is it important?" I cannot sit here and say that it could never be important. And I doubt very much that anybody can sit here and tell us that it is always important.

All I can do, aside from offering you my subjective evaluation by saying it is important, very important, not too important, or not important at all, is to tell you that in no case that I have listed in that memorandum to you was either consensual or non-consensual eavesdropping used.

Now, I confined the thrust of my statement to nonconsensual, but I amended it to tell you that in none of the cases I have enumerated was even consensual eavesdropping used.

It seems to me it is reasonable for you to judge, based on objective fact, the importance or lack of importance that you would ascribe to consensual eavesdropping.

The fact of the matter is that from time to time it can be a very useful thing. I will not sit here and say otherwise. But how important is it in the eyes of the beholder?

In any event, as I understand the lawsuit, the Supreme Court has held clearly affirmatively that consensual electronic recordings do not violate any right to privacy as contemplated by the Fourth Amendment of the United States Constitution.

Am I correct on that?

MR. REMINGTON: I understand that, but there is a policy Professor Blakey referred to, and that is even though it's not constitutionally required, whether as a matter of public policy consensual overhears, et cetera, ought to be prohibited or ought to be subjected to a warrant requirement.

And in attempting to respond to that, one aspect of the question is: How important are they? Because it seems to me if they are unimportant, it is much easier to either increase the requirements or prohibit their use than it is if the conclusion is that the authority to do this is very important.

MR. STERN: It seems to me that that is an interesting policy question, but the first question you should ask is: Is there any right to privacy at all in the area? Because you don't need to get into the balancing task if there isn't a right to privacy.

MR. REMINGTON: My memory is that four members of the Supreme Court thought there was.

MR. STERN: Yes. But unfortunately, until they can collect a fifth vote, there isn't.

MR. REMINGTON: If you take the position that decisions on these matters ought to be left solely to the judicial system—and I think myself that conclusion is appropriate—but if one takes the position that important public policies ought to be dealt with by the legislative branch, then I think that if only four members of the Supreme Court feel that way, that doesn't make it so.

MR. STERN: When you get into the area of evaluation, my evaluation, which is as good as anybody else's, is not based on expertise but based on

my own concept of what a right to privacy is or isn't. I think anybody who has been in enforcement can give you their experiences in terms of what has been a useful technique or a not useful technique. In terms of their subjective evaluation of what is private and what is not, they stand in no special position.

I cannot see where either one has a right to privacy as opposed to the other one, unless, of course, you have a situation where A and B have contracted with each other that what is said will not be otherwise disclosed. I cannot see why either one doesn't run the risk, absent such agreement, either express or perhaps implied, or why either one has the right to complain if the other one repeats what is said. And if one can repeat what is said, I can't understand why one cannot repeat verbatim what is said. And if one can repeat verbatim what is said, I can't understand why one cannot furnish the best evidence of what is said, the actual recording.

If you are saying B has no right to record what A said, the question arises: Why has he any right to testify as to what A says? And it seems to be in making the determination about consensual recordings in this area, you have to make the decision: If the recording of the actual words of A is a breach of privacy, why isn't the repeating of A's statement from memory the same kind of breach?

MR. REMINGTON: I take it your testimony is that a consensual overhear ought to be recognized as lawful, regardless of whether it is regarded as needed or not; that it is so minimal an invasion of privacy that this Commission really ought not consider the question of whether it is necessary; that we don't have to go through a balancing process because there is no loss of privacy in the use of this particular enforcement method.

MR. STERN: I think I agree with that proposition. I can't see the distinction between recording it and permitting B to repeat what A said to him—if that does not breach A's privacy. And if it does, you can effectively close down all prosecutions in this area.

I think all would agree one indispensable ingredient to all these prosecutions of corrupt politicians or people in the public service would be the real live testimony of somebody getting on the stand and testifying that he dealt with that man or paid him money or what the man said to him.

If he can do that, why couldn't he surreptitiously take a photograph of himself paying the money? Why couldn't he record the words?

I just don't see the issue.

MR. REMINGTON: Thank you.

CHAIRMAN ERICKSON: Judge Shientag.

MS. SHIENTAG: Judge Stern, you have been sitting in the District Court for a year and a half?

MR. STERN: Yes.

MS. SHIENTAG: And you have had extensive experience both in New York and New Jersey.

Has any application come before you as a judge for wiretapping?

MR. STERN: No, ma'am.

MS. SHIENTAG: You have made a value judgment about wiretapping which is well known.

MR. STERN: Pardon me?

MS. SHIENTAG: You have come to a conclusion about the moral right to have wiretapping.

MR. STERN: I don't think I have testified to that here. Do I have an opinion on it? Yes, I have an opinion on it.

MS. SHIENTAG: And what is your opinion?

MR. STERN: Well, I for one cannot see why it is that if one can show probable cause to believe a specific man is committing a specific crime using a telephone—I don't see any vested right in that man to commit that crime by use of the telephone in private.

My morals are not shocked by denying him a private dispatch case under those kinds of circumstances. Neither were the morals of Congress which passed the statute—

MS. SHIENTAG: How do you feel about the right to privacy, then?

MR. STERN: It is an important right.

MS. SHIENTAG: It is very important in respect to human beings.

MR. STERN: Absolutely.

MS. SHIENTAG: And since no applications have been brought before you, would you assume that most officers know of your opinion?

MR. STERN: It doesn't work that way in my court. First of all, I have been on the court a year and a half, and I came from the U. S. Attorney's office. And my rule is that I will not take any case unless the crime was committed after I left the U. S. Attorney's office.

So first of all, at least for the time being, until I get a little more remote from these investigations so the appearance of impropriety won't appear, that effectively limits some of the things I will do.

Secondly, the prosecutor in our district does not choose the judge he will go before. It is a secret list—a rotating list. The prosecutor doesn't know who the judge will be.

MS. SHIENTAG: So there isn't any shopping around?

MR. STERN: No. We don't want to let them do that because we don't think it's fair.

MS. SHIENTAG: Because it has been said there is shopping around for a judge who will be favorable to wiretapping.

MR. STERN: I can only report to you the situation in my district.

MS. SHIENTAG: It doesn't exist in your district?

MR. STERN: To the best of my knowledge and belief, the clerk of our court keeps a list—the same way we are on an individual calendar system for indictments. The indictment comes out of the grand jury and the next judge gets it.

And as a matter of fact, in order to preserve the integrity of the process, it isn't done on a rotating basis, in other words, Judge 1, Judge 2, Judge 3, Judge 4, and Judge 5, because you could predict then.

What happens is there are a number of cards. Each judge may have 20 cards with his name on them which are put in a bundle, and the cards are pulled from the pack. And this equalizes out but no one can predict in advance which judge will take which case.

MS. SHIENTAG: Would you suggest that as a means of avoiding what has been characterized as shopping around in other districts?

MR. STERN: It works in ours. I hate to be in a position of telling my colleagues in other places what to do. I am sure they are all concerned, as we are concerned, with avoiding even the appearance of judge-shopping.

MS. SHIENTAG: Just a few more questions.

Take any one of the cases that is set forth in your statement to us—any one of those cases.

MR. STERN: Jersey City. Let's take Jersey City.

MS. SHIENTAG: That is on page 2 of your statement.

In that case there was an indictment you helped secure, and I suppose you helped try the case.

MR. STERN: I personally tried it.

MS. SHIENTAG: There was a conviction against the Mayor, the President of the City Council, the Business Administrator, and numerous other officials.

To make that case, did you use physical surveillance?

MR. STERN: No, ma'am.

MS. SHIENTAG: Did you use grand jury sanctions?

MR. STERN: What do you mean by "sanctions?"

MS. SHIENTAG: Did you have someone appear before the grand jury and have them testify and grant them immunity?

MR. STERN: Yes. People appear before the grand juries. We cannot under the Fifth Amendment of our Constitution return an indictment without his appearing before a grand jury.

MS. SHIENTAG: Did you grant immunity to get cases on higher-ups?

MR. STERN: Yes.

MS. SHIENTAG: Did you have cases against defendants?

MR. STERN: People who were witnesses?

MS. SHIENTAG: People who were defendants and made confessions to testify against other persons.

MR. STERN: If they became witnesses—not to quibble, but I don't understand.

If a possible defendant elected to become a government witness—we have such. If you mean do we have a confession from somebody who was indicted and read it in at the trial, the answer is no.

MS. SHIENTAG: Did you use photographs of any of the defendants together?

MR. STERN: No. Would you like to know how we did it?

MS. SHIENTAG: I'd like to know how you made that case which was a very tough case.

MR. STERN: Well, for 50 years in Hudson County and Jersey City, everybody said it was corrupt, from Frank Hague down through John V. Kenny. Indeed, the story was—and every cab driver knew it—that you couldn't do business in Hudson County without kicking back 10 percent. Indeed, that community coined the phrase “way of life,” and I put quotes around it.

It was our theorem that if it was that notorious, it ought to be easily discoverable, and we decided to apply a certain technique we had learned in the Colonial Pipeline case.

I know the former Attorney General Ramsey Clark is here to testify. I worked under General Clark and had the privilege of using one of his letters of immunity.

So we decided to test the theory and see whether or not we could prove that everybody who did business in Jersey City had to pay off.

So the first thing to do was to find out who did business in Jersey City. So we subpoenaed out of the City Hall and the Administration Building every single contract awarded to engineers and contractors in the past five years in an amount over \$2,500.

That gave us, as you can imagine, literally hundreds and hundreds of thousands of documents.

From those records, we determined who the successful awardees of public contracts had been, and we then subpoenaed in all of their books and records.

And we used two theories.

Theory No. 1 was a crooked public official does not take a payoff by check. It has got to be cash.

Theory No. 2, very rarely in our society today does somebody go to the bank and cash a \$20,000 check or a \$10,000 check and walk out with greenbacks for a legitimate purpose.

So it then became an accounting function to check through the books and records of the businessmen who had done business with Jersey City

and Hudson County, in an attempt to ascertain whether there were large amounts of cash coming out.

When we found those large amounts of cash, the next step was to bring in the appropriate businessman and ask him what he had done with the cash.

Most often, of course, you'd encounter the invocation of the Fifth Amendment because under our system of laws you cannot compel a man to give evidence which could possibly incriminate himself, because money paid from a businessman to a public official is incriminatory. We'd then utilize the immunity laws, and in that way we developed the evidence.

MS. SHIENTAG: So you granted immunity after having seized the books, by warrant, I assume?

MR. STERN: No.

MS. SHIENTAG: How did you get the books?

MR. STERN: Subpoena *duces tecum* of a grand jury.

MS. SHIENTAG: And the persons testified under a grant of immunity.

MR. STERN: Ultimately, yes.

MS. SHIENTAG: As to the contents of the records?

MR. STERN: No. You don't need to give immunity for that. Technically, under the law, if it is a corporation they have to bring it in. There is no Fifth Amendment right there.

MS. SHIENTAG: You only proceeded against corporate defendants or corporate suppliers?

MR. STERN: Some were small partnerships but some were very large. One was a division of Ashland Oil which paid a considerable sum. There were a number of large contractors.

But the point is that once you find the cash—you see the bribery usually takes place in private between two people who don't do it on a street corner. And you are never going to make that case without the testimony of one of them. And under our Fifth Amendment, you can't compel a man to be a witness against himself.

So the immunity laws, under those circumstances, if you want to have a strong and vital Fifth Amendment, which I think is fundamental—you have to have immunity laws or you are really giving benefit to two men who lock themselves alone in a motel room and exchange cash.

MS. SHIENTAG: Would it not have been easier had you been able to use a recorder on one of the persons?

MR. STERN: No. Almost all of the transactions had taken place, if not months before, then years before. And the very method of obtaining the testimony virtually required that the crime be already completed.

It was not our experience, you see, that businessmen came flocking down to us when they were solicited for money. Nor was it our experience that public officials came trooping down to our office to report that graft was being taken by their colleagues.

It was uncovered on the basis of a completed crime which we unraveled from the books.

MS. SHIENTAG: There has been testimony before us, Judge Stern, that as to ongoing crimes of corruption, too, it is very valuable to have a recorder available or to use a telephone.

MR. STERN: The problem again is one of definition of terms. I tried, ma'am, to delineate out earlier that I was not talking about a bookmaker paying off—

MS. SHIENTAG: No, I am talking about corruption, just as in your case. We have had testimony before us to that effect.

Do you think the distinction possibly could be as to ongoing crimes and cases which took place long before, as in the case of the Jersey City case you described.

MR. STERN: It is difficult for me to answer, ma'am, without knowing what the previous witness referred to.

MS. SHIENTAG: That is true. But have you ever had a case where the crime was ongoing rather than completed?

MR. STERN: Yes.

MS. SHIENTAG: And you didn't find it necessary, in order to make your case, to use any electronic surveillance?

MR. STERN: No. And that is not so in all cases, ma'am. In a few cases, as I indicated earlier, there were consensual recordings made.

In other words, where a businessman came in and said, "Look, X public official has asked me for money, and I have to make a payment, and I don't want to make a payment"—in some of these cases, the person wore a recording device and actually recorded the public official taking the money. There were a very small number of those.

MS. SHIENTAG: Generally, would you say that you would not disapprove a consensual wiretap in an ongoing case, a current case?

MR. STERN: You mean consensual eavesdropping?

MS. SHIENTAG: Eavesdropping.

MR. STERN: I don't disapprove it. I did, in fact, approve it.

MS. SHIENTAG: You approved it?

MR. STERN: Yes.

MS. SHIENTAG: Thank you.

CHAIRMAN ERICKSON: Chief Andersen.

MR. ANDERSEN: Judge Stern, in your definition of political corruption, may I ask you, did you classify judiciary corruption as political corruption?

MR. STERN: Yes. I think the man who sold out the second circuit and went to jail for it—when I say political I mean somebody in public office.

MR. ANDERSEN: An elected and/or appointed official?

MR. STERN: Yes, in any of the three branches which I think I indicated earlier.

MR. ANDERSEN: As to your definition—the New Jersey prosecutors testified that there was a statewide grand jury concept, and they have had over 150 indictments in three years, and they have used wiretapping very extensively, it is my understanding from their testimony—do you see a conflict in your thinking and their thinking? Or is it your position that they could have made all these cases without electronic surveillance?

MR. STERN: Well, I don't know what cases they were referring to, but they obviously weren't referring to the cases I was referring to in New Jersey. And you can take a list of the cases I presented for you of New Jersey cases made without it, and I would suggest you get their list and see what kind of corruption cases they are referring to.

I would suspect from the numbers I have just heard from you, Mr. Andersen—I don't know; I am at a disadvantage because I wasn't here for the testimony—I suspect they are discussing police payoffs.

What I was trying to explain to Miss Shientag a moment ago was that when you have a local bookmaker who is paying \$100 a month to a policeman every month to stay in business, it may be that kind of ongoing, continuous, organized, if you will, payments, are susceptible to that kind of investigative approach.

But I worked in New Jersey—I don't know who testified here, but I probably worked alongside some of the people who testified here, I on the Federal side and they on the state side. And I can point to what I did.

MR. ANDERSEN: You are probably recommending that we should compare the two, and the level of cases, and you are saying there is probably not a conflict in the two concepts. Would that be a fair evaluation?

MR. STERN: I am saying if you compare them you may find an essentially different kind of emphasis on the prosecution of essentially different kinds of crimes.

MR. ANDERSEN: I have no further questions.

CHAIRMAN ERICKSON: Thank you.

I have just a couple of wind-up questions, if I may, Judge.

Regarding the Knapp Commission work in New York, the use of consensual eavesdropping equipment in that type of investigation is more or less essential, don't you feel?

MR. STERN: Where you are fortunate enough in any kind of corruption case, whether you view it as the police lieutenant or the captain or the inspector taking money, or the mayor taking money—if you are fortunate enough to find out about it while it's midstream, then obviously you can do something useful with electronic surveillance.

My main thrust is that in the area of not the local police corruption so much as in the area of a congressman who takes graft, or a mayor, that kind of thing, you generally don't find out about it midstream, and that has generally been my experience and, as far as I can ascertain from most of my colleagues when I was in the United States Attorney's office, their experience in those types of cases.

CHAIRMAN ERICKSON: Judge Stern, we are very grateful to you for the testimony you have given. It will be helpful to us in preparing recommendations to the Congress and to the President, and you have furnished a very high service to us in giving us your time and effort.

Thank you very much.

MR. STERN: It is a pleasure to be here.

Thank you.

CHAIRMAN ERICKSON: At this time, before calling our next witness, we will take a brief recess. But before recessing I would advise the Commission that I have just been delivered a letter from the Attorney General advising us that he will submit a formal statement to us in response to the questionnaire that was sent to him, and that before answering the questionnaire he will confer with a number of United States Attorneys who will be meeting here in Washington on June 17.

His letter will be filed as part of the record. His new commitments, since taking office as Attorney General, are such that it was impossible for him to appear and give testimony.

I believe his report will be helpful, and we are looking forward to receiving it.

At this time we will take a ten-minute recess.

[Whereupon, a short recess was taken.]

[The letter of Attorney General Edward H. Levi follows.]

Office of the Attorney General

Washington, D. C. 20530
July 30, 1975

Honorable William H. Erickson
Chairman

National Commission for the Review of Federal and State Laws
Relating to Wiretapping and Electronic Surveillance
1875 Connecticut Avenue N.W.
Washington, D. C.

Dear Mr. Erickson:

This is in further reply to your letter of May 23, 1975, inviting me to express my thoughts with regard to court-authorized electronic surveillance.

I note that the Department has already provided extensive views to the Commission. On September 16 and 17, 1974, statements and testimony were presented by the Attorney General, William B. Saxbe; Assistant Attorney General, Henry E. Petersen of the Criminal Division; Clarence M. Kelley, Director of the Federal Bureau of Investigation; and John R. Bartels, Jr., Administrator of the Drug Enforcement Administration. I generally concur with the views which Messrs. Saxbe and Petersen expressed in their formal statements, and have only the following few additional observations to set forth.

Although statistics over the past six years have shown that the use of oral, as distinguished from wire, consensual monitoring by the investigative agencies has progressively increased, there has been an acceleration in the rate of increase since Mr. Petersen provided statistics to the Commission last September. At your request, Mr. John C. Keeney, Acting Assistant Attorney General, provided supplementary figures which reflected the increase in oral consensual monitoring through March 1975. I am enclosing additional figures which reflect similar information for the months of April through June 1975.

The recent increase in consensuals appears to be attributable primarily to three factors: an increase in the number of investigations in which oral consensual monitoring is usually employed, agency encouragement of the use of consensual monitoring techniques, and the influence of technical considerations, such as the improvement of techniques and the acquisition of additional or more advanced equipment.

The most dramatic increase in consensual monitoring has been reported by the Drug Enforcement Administration. This agency has been encouraging its agents to utilize consensual monitoring equipment to minimize assaults on its undercover personnel, 300 of which have occurred during the past eighteen months. To support its operations, it has been procuring additional as well as improved consensual monitoring equipment and has recently established a technical operations field program to train agents in the use and maintenance of the equipment.

The Federal Bureau of Investigation has recently placed increased emphasis on the investigation of white collar crime, particularly bribery, fraud, and embezzlement, in which corroborating evidence obtained through consensual monitoring is crucial to the success of the investigation. The Bureau has also been employing undercover techniques where the maintenance of a communications link by consensual monitoring is essential for the protection of the undercover agent.

Other investigative agencies attribute their increase in consensual use to a greater number of investigations involving the employment of electronics to maintain communications contact in undercover operations both for the protection of agents and to coordinate the actions of monitoring agents with those of undercover operatives.

I appreciate the opportunity of presenting my views. I look forward to reading the Commission's report.

Sincerely,

[Signed] Edward H. Levi
Attorney General

Enclosure

**AGENCY REQUESTS FOR CONSENSUAL
MONITORING AUTHORITY**

Month	Year	Regular	Emergency	Denied	Total
Sept.....	1974	95	145	0	240
Oct.....	1974	106	139	0	245
Nov.....	1974	108	208	1	317
Dec.....	1974	131	158	0	289
Total for year.....	1974	1,221	973	6	2,201
Jan.....	1975	118	208	0	326
Feb.....	1975	135	202	3	340
Mar.....	1975	161	300	0	461
Apr.....	1975	150	91	0	241
May.....	1975	175	405	0	580
June.....	1975	171	456	1	628
Semitotal for year.....	1975	910	1,662	4	2,567

CHAIRMAN ERICKSON: Ladies and gentlemen, may we reconvene. We are going to try to keep from taking advantage of the time of our witnesses. We know they have schedules they are trying to meet.

We are particularly honored to have the Honorable Ramsey Clark with us this morning. He is the former Attorney General of the United States under the administration of President Lyndon Johnson. He was the Attorney General when the wiretapping statute was enacted in 1968, but he was opposed to the use of nonconsensual electronic surveillance in law enforcement, and no wiretap orders were obtained until his successor took office in 1969.

Mr. Clark is now engaged in the private practice of law in New York, and I am certain all of you are aware of the practice and work that he has done in improving the administration of justice.

General Clark, would you be sworn?

[Whereupon, Mr. Clark was sworn by Chairman Erickson.]

**TESTIMONY OF THE HONORABLE
RAMSEY CLARK, NEW YORK, NEW YORK**

CHAIRMAN ERICKSON: Do you have a prepared statement?

MR. CLARK: I do not have a specially prepared statement. I have a statement that I used before the Senate Judiciary and Foreign Relations Committees last year, and there are just parts of it—I will leave a whole copy with you, but there are parts of it that I thought might be helpful to your Commission this morning.

CHAIRMAN ERICKSON: It will be made part of the record.

[The statement of Ramsey Clark follows:]

**STATEMENT OF RAMSEY CLARK
before the
CONSTITUTIONAL RIGHTS SUBCOMMITTEE
ADMINISTRATIVE PRACTICE AND
PROCEDURE SUBCOMMITTEE
of the
COMMITTEE ON THE JUDICIARY
and the
FOREIGN RELATIONS SUBCOMMITTEE ON
SURVEILLANCE
of the
FOREIGN RELATIONS COMMITTEE
of the
UNITED STATES SENATE**

Wednesday, April 3, 1974

Be warned of my bias against wiretapping and electronic surveillance. I believe it to be far more than a mere dirty business. It tinkers with the foundations of individual integrity. A nation that embarks on such a road, approving inherently immoral acts by government, will come to a time when it wiretaps nonviolent leaders of social change, the offices of the opposing political party and finally the President's brother.

Your committees will need to study thoroughly the use of electronic surveillance by government if you are to decide wisely and achieve needed prohibitions and controls. Sadly, our ignorance exceeds our knowledge of such subjects because we practice government by secrecy. This is dangerous for a people who would be free and makes democracy unworkable. But here we are.

Let me give some of the history of wiretapping and electronic surveillance as I know it. The beginning was small. The Bureau of Investigation was created in the Department of Justice in 1924. In February of 1931, at a time when the regulations of the Bureau of Investigation provided that wiretapping would "not be tolerated," Mr. Hoover disclosed that he knew of only three wiretaps during its history. Reminiscent of a sad dispute in the late 1960's, he explained he did not discover two of them until long after they occurred. As to the other one, he was instructed by the Attorney General of the United States to undertake the activity. The wiretaps were on matters of essentially no importance. The first one occurred in 1926 in Indianapolis, Indiana, in connection with an investigation under the Packers and Stockyards Act. The investigation itself was aborted. Two years later, Mr. Hoover found out the wiretap had been initiated.

The second one had to do with an investigation of administrative irregularities at Leavenworth Penitentiary, where you should hardly need a wiretap to find out what prison officials were doing if you had any integrity in your institution.

The third one involved the Department of Justice itself. It seems that Attorney General Sargent heard that it was possible to call certain phone numbers in the Department of Justice and order alcoholic beverages. This was during prohibition. A wiretap was put on those phones to see whether the allegations were true.

From 1924 to 1931, there was only one other investigative agency in the Department of Justice, the Bureau of Prohibition, which enforced the prohibition laws. It apparently engaged rather freely in wiretapping, which gives you some sense of the priorities and importance that have been attached historically to this sort of business.

In the fall of 1931 Attorney General Mitchell—William D. Mitchell—authorized the Bureau of Investigation to use wiretaps over the objection of Mr. Hoover, "... where the crimes are

substantial and serious, and the necessity is great, and they are satisfied that the persons whose wires are tapped are of the criminal type." He further said, "It is expected . . ." that authority will be given.

The next significant reference to wiretapping that I recall from Department of Justice records arose from a dispute involving a prosecution in the city of Baltimore by the State of Maryland under its prostitution ordinances. Apparently, the FBI used wiretaps in a federal investigation under the Mann Act and turned information obtained from it over to the State for prosecution. A small scandal arose, as it should have.

In 1939 as World War II approached, legislation was proposed to authorize wiretapping. Mr. Hoover, who by then had directed the FBI for 15 years, said he thought wiretapping was "of very little value" and that the risk of "abuse would far outweigh the value."

In March of 1940 Attorney General Robert H. Jackson, on the basis of an oral instruction followed later by a written order from President Franklin Roosevelt, advised the U. S. attorneys around the country that wherever wiretapping was employed, there was to be absolutely no use of any information gathered in any grand jury investigation or other prosecutorial effort.

On May 21, 1940, President Franklin Roosevelt signed his now famous order to Attorney General Robert H. Jackson concerning wiretapping. President Roosevelt said he agreed with the broad purpose of the Supreme Court decision in the *Nardone* case, but could not think, and he was of course right, that the court was then considering the risks the country faced from international conflict. Therefore, where there was substantial risk of international violence, "grave matters involving the defense of the nation," or subversion, he was ordering the use of wiretap. "It is too late to do anything about it after sabotage, assassinations and 'fifth column' activities are completed," he argued. He said in the last paragraph of his letter that it should be limited to the "minimum" and limited "insofar as possible to aliens."

The scope of the use of electronic surveillance during the war is difficult to determine. Some indication of FBI use just before the war is given by the following. Between September 2 and October 2, 1941, in the months just before Pearl Harbor, the Federal Bureau of Investigation asked Attorney General Francis Biddle to authorize seven wiretaps. Two were on persons who had some relation to Germany. One was an office, the German commercial attache in New York City. Another was on a German citizen who had an automobile with a shortwave radio in it who drove around this country and down into Mexico.

Two had to do with Japanese. One was placed on the Japanese consulate at San Francisco, the other was to monitor all telephone calls from Hawaii to Japan. That request was made September 2, 1941.

The other three all involved alleged Communists. One was a young woman in San Francisco, one was a man who lived in North Hollywood, California, and the third—and this tells you much you need to know—was a book store in Philadelphia. All but one of the wiretaps, the bookstore in Attorney General Biddle's Philadelphia, were authorized. Most requests were pending for over a month before they were authorized.

In July 1946 Attorney General Tom Clark, consistent, he said in his memo to President Truman, with the acts of his two immediate predecessors, sought and obtained authority to tap in areas ". . . vitally affecting domestic security." This was at the beginning of the so-called cold war.

President Eisenhower's first Attorney General, Herbert Brownell, affirmed and expanded that general authority to wiretap in the 1950's.

The use of electronic surveillance against organized crime apparently began in the late 1950's while William P. Rogers was Attorney General. I am not aware of any documentary evidence that he knew of or authorized such surveillance. This activity expanded during the 1960's until 1965. Robert F. Kennedy denied

that he authorized or knew of this electronic surveillance. I believe him.

By June 30, 1965, there were extensive patterns of use in domestic and national security areas. The requests for wiretaps in the national security area came primarily from the National Security Council, the National Security Agency, the Department of State, and from the FBI. On June 30, 1965, President Lyndon B. Johnson sent a memo to all heads of executive departments and agencies which began "I am strongly opposed to the interception of telephone conversations as a general investigative technique." He required all wiretaps within the United States to be approved by the Attorney General, and that approval be given only in "investigations related to the national security." This ended the general use of wiretaps outside the national security area through the end of the Johnson Administration. I do not know what wiretapping by our Government goes on outside the United States and urge you to explore this too.

I became acting Attorney General in late September 1966 when Nicholas Katzenbach was nominated to the Under Secretary of State. At that time I was not informed of wiretaps that had been theretofore approved. Nor did I find any evidence that former Attorneys General maintained lists of approved surveillance from which they could determine how many and where wiretaps were being employed at any given time.

By November of 1966 I had discussed and developed a regular reporting technique with Mr. Hoover. In December of 1966 I was given a listing of all electronic surveillance currently authorized and in use. Each quarter thereafter I was given an accounting of the number of wiretaps and other electronic surveillance in place at the beginning of the preceding quarter, the number of new installations and discontinuances in the quarter and the number in place at the end. This practice continued through my tenure as Attorney General.

As you will recall, I opposed wiretapping as Attorney General. On March 20, 1967, I appeared before the Subcommittee on Administrative Practice and Procedure urging enactment of the Right of Privacy Act of 1967 (S. 928) and testified:

"We cared enough for our privacy to prohibit unreasonable searches and seizures and unrestricted warrants in the Bill of Rights. For privacy is after all the foundation of freedom and the source of individualism and personality. But as Justice Brandeis observed nearly four decades ago ' . . . general warrants are but puny instruments of tyranny and oppression when compared to wiretapping.' Still we permit the most insidious invasion of privacy—the electronic surveillance.

"Nothing so mocks privacy as the wiretap and electronic surveillance. They are incompatible with a free society and justified only when that society must protect itself from those who seek to destroy it.

"Only wiretapping and eavesdropping directly related to and necessary for the protection of the security of the Nation is excepted from the prohibitions contained in the bill. Even in this narrow area, however, no information obtained as a result of such measures will be admissible in evidence in judicial or administrative proceedings. Other use or disclosure of such information is prohibited except as essential to national security. The national security exception is a necessary provision in the statute; the evidentiary restrictions, however, will serve an important function in confining such activity to the extremely narrow bounds that are appropriate."

After Title III of the Omnibus Crime Control Act of 1968 authorized the use of wiretap in domestic crime, I publicly declined to use the authority. This, in addition to my public opposition to wiretap, became an issue in the 1968 Presidential campaign. John Mitchell, appearing before the Judiciary Committee at his confirmation hearing to be Attorney General on January 14, 1969, was reported by *Time* magazine to have promised the Committee he would "use electronic devices for national security and against organized crime" and further reported that I "had brusquely refused to use wiretapping."

Wiretapping in the national security area continued while I was Attorney General. Then as now I doubted its real value and oppose even this use. It will be many years in my opinion before we muster the wisdom and courage necessary to prohibit this use.

I do not believe any wiretapping or electronic surveillance was authorized or utilized outside the national security area while I was Attorney General. Every installation approved involved a foreign nation, its embassy, or other office, its personnel or agents, or persons allegedly acting directly in the behalf of a foreign nation. The numbers of wiretaps approved is not clear to me, but I have some evidence that on November 23, 1966, the day of the first accounting, there were 107 wiretaps or electronic surveillances on foreign missions and persons or alleged agents. I endeavored to reduce these numbers and by December 27, 1966, there were 76 wiretaps and electronic surveillances. By March 27, 1967, there were 44 such surveillances. The numbers remained fairly constant and on December 24, 1968, the last accounting while I was Attorney General, there were 43 wiretap and electronic surveillances. The numbers of new wiretaps approved and old ones discontinued were few in any accounting period. Some of the wiretaps had probably been in use for decades. There was in addition electronic coverage of from 40 to 50 teletype machines in various foreign missions.

Throughout the time I was Attorney General applications for wiretaps in the domestic area were presented to me. I did not discourage this because I could not foresee what circumstance might arise, and there was a long history of approving such surveillance. No domestic surveillance was approved by me while I was Attorney General.

Examples of requests to wiretap which I rejected, and some on several occasions, were Martin Luther King, Jr., Southern Christian Leadership Conference, African-American Heritage Association, Student Non-Violent Coordinating Committee, Stokeley Carmichael, H. Rap Brown, Leroy Eldridge Cleaver, Fred Allen Hampton, the Black Panther Party, Robert Alfonso Brown, Demonstrations at the Democratic National Committee (first requested and rejected March 12, 1968), Students for a Democratic Society, Student Mobilization Committee, Fifth Avenue Peace Parade, Jerry Rubin, National Mobilization Committee to End the War in Vietnam, and Liberation Magazine.

In tightening approval of national security wiretaps I sought to confine the area of approval to international activities directly related to the military security of the United States. This caused the disapproval of many applications to wiretap in the foreign field. Examples would include the denial of a request to tap Abba Eban when he was on a visit to this country, an employee of the United Nations Secretariat, the Organization of Arab Students in the U. S., the Tanzanian Mission to the U.N., the office of the Agricultural Counselor at the Soviet Embassy and a correspondent of TASS.

Once Mr. Hoover, apparently at the request of the National Security Agency, sought approval to break and enter into a foreign mission at the United Nations to procure cryptographic materials to facilitate decoding of intercepted transmissions. The request was presented with some urgency, rejected and presented again on perhaps several occasions. It was never approved and constituted the only request of that kind.

Since I left office, we have seen Attorney General John N. Mitchell claim an inherent executive power to wiretap in the domestic area without a court order. This dangerous and lawless claim was rejected by the U. S. Supreme Court in the *Damon Keith* case. We have also heard of wiretaps on government officials, newsmen, and others. While President Nixon has said his administration has done less warrantless wiretapping than its predecessors, we do not know. I do not believe him.

Your committees must require a full accounting from the executive. You and the people are entitled to know the whole history and practice of this sordid business. I urge you to demand

full disclosure and if cooperation is not extended, to seek power to subpoena the records and personnel that can fully inform you. It will be necessary to know as well whether unauthorized wiretapping has been engaged in by federal agents. I do not believe this happened to any significant degree while I was Attorney General. We must also know whether state, local or private agents have been induced to wiretap by federal agencies.

From the knowledge thus gained you will have a rational opportunity to measure the value and necessity for wiretapping. If you do this, I believe you will prohibit all wiretapping and cause the files of government containing information from wiretaps to be purged.

In the meantime, I believe you should require all wiretaps to be approved by a judicial officer. National Security wiretapping should be limited to matters directly and substantially affecting the military security of the United States from foreign sources. Domestic wiretapping should be limited to violent crimes and Fourth Amendment protection should apply as if the act were a search and seizure. All wiretap and electronic surveillance should be reported regularly to the Administrative Office of the U. S. Courts, the appropriate committees of the Congress and the people with full disclosure of time, place, persons involved and reasons for the surveillance as soon as practicable after the fact. If we are to be a government of laws, you as lawmakers must face your responsibility to know what agents of the United States do in its name, to set the rule and see that it is followed. Finally Congress must evaluate the information obtained and hopefully decide the practice is not worth the price we pay in public morality.

CHAIRMAN ERICKSON: In order to put our Commission on the proper plateau, we would welcome some opening remarks.

MR. CLARK: Thank you very much. It is a privilege to be here, Mr. Chairman, and members of the Commission.

It is hard to talk about freedom and remember the long history of this country these days, and how we have grown in freedom, because it is a complex time and we tend to be afraid of so many things.

But I would urge you, as we approach our 200th birthday, not to forget what I consider to be the single most important principle in the history of this country—freedom—and study the relationship of wiretapping and electronic surveillance to freedom with great care.

Mr. Chairman, you asked Judge Stern a question about the Knapp Commission just at the end of his testimony, and whether wiretapping wasn't essential to its performance.

I had some familiarity with the Commission and had the great honor of representing Frank Serpico before the Commission and otherwise, and I can tell you something that is a lot better than wiretapping in a situation like that: It is an honest cop. If you want an opinion, at least as to where the information that had the greatest value and the most effect came from, it wasn't from wiretaps or anything like that—it was from honest cops. There is no substitute for them, and never will be.

We forget our history, and I think there is enough change that we will not be likely to repeat it. Our future may not be that happy. But there is still some relevance to history and I'd like to go through briefly some of the history of the use of wiretapping in the United States Department of Justice.

While I was Attorney General I caused a listing to be made, as best as we could, from the files that were available to the Office of the Attorney General, and I'd like to run down the beginnings of the use of wiretap. They may sound quaint, but we are talking about events within lives in being, and they show how dangerous it becomes to get so deeply in the forest that you can only see the trees.

The beginning was small. The Bureau of Investigation was created in the Department of Justice in 1924. In February of 1931, at a time when the regulations of the Bureau of Investigation provided that wiretapping would "not be tolerated," Mr. Hoover disclosed that he knew of only three wiretaps during its history. Of course, Mr. Hoover had headed the Bureau of Investigation, later to become the FBI, from its creation, and he was saying that over those seven years he had discovered the existence of three wiretaps.

It is pretty interesting to see what they were. It tells us something about motivations and how we tend to employ them today.

The first one was reminiscent of a sad dispute in the late 1960's. Mr. Hoover had to explain he did not discover two of them until long after they occurred. Many more recent Attorneys General have been severely taken to task because with the Bureau having 7,700 agents and engaging in more than 700,000 investigations a year, they didn't know everything that the FBI was doing. Here was the Director of the FBI in a very simple time, where he knew each agent, and he only learned years after they occurred of two of the three wiretaps that were in place in the first years of the Bureau.

And as to the third one, he was instructed by the Attorney General of the United States to undertake that activity specifically, so he learned in advance of it. The wiretaps were on matters of essentially no importance. The first one occurred in 1926 in Indianapolis, Indiana, in connection with an investigation under the Packers and Stockyards Act. Nothing happened. Two years later Mr. Hoover found out the wiretap had been initiated.

The second had to do with an investigation of administrative irregularities at Leavenworth Penitentiary, where you should hardly need a wiretap to find out what prison officials were doing. If you have any integrity in your institution, that is not any way of instilling integrity into the personnel of a penal institution or any institution.

The third one involved the Department of Justice itself, as did the second. It seems that Attorney General Sargent heard it was possible to call a certain phone number in the Department of Justice in Washington, D. C. and order alcoholic beverages in violation of law. This was during prohibition. A wiretap was put on these phones to see whether the allegations were true.

From 1924 to 1931, there was only one other investigative agency in the Department of Justice, the Bureau of Prohibition, which enforced the prohibition laws, and apparently engaged freely in wiretapping.

And in the fall of 1931, Attorney General William D. Mitchell authorized the Bureau of Investigation to use wiretaps over the stated objection of Mr. Hoover, "where the crimes are substantial and serious, and the necessity is great, and they are satisfied that the persons whose wires are tapped are of the criminal type."

He further said, "It is expected" that authority will be given, under questioning.

The next significant reference under that authorization in 1931, over Mr. Hoover's objection, that I have been able to cut out from the Department of Justice records, arose from a dispute arising in the City of Baltimore by the State of Maryland under its prostitution ordinances. Apparently the FBI used wiretaps in a Federal investigation under the Mann Act and turned the evidence over to the state for prosecution. Apparently a small scandal arose, as it should have.

We are approaching World War II. My judgment is that the extent and power of organized crime in the United States reached its height in the '20's and '30's. We can remember a single day in, I think it was February 1931, when 41 people were shot down in the street in a single organized crime battle. That is not saying there is not more organized crime than there ought to be, but it's simply saying that things have been as bad or worse in the past when we weren't using wiretaps.

During 1939, legislation was proposed to authorize wiretapping. Mr. Hoover, who by then had directed the FBI for 15 years, said he thought wiretapping was "of very little value" and that the "risk of abuse would far outweigh the value."

In March of 1940 Attorney General Robert H. Jackson, on the basis of an oral instruction followed later by a written order from President Franklin Roosevelt, advised the U. S. Attorneys around the country that wherever wiretapping was employed, there was to be absolutely no use of any information gathered in any grand jury investigation or other prosecutorial effort, which hopefully had been a constitutional right for sometime before that, at least in Federal prosecution.

On May 21, 1940, Franklin Roosevelt signed his now famous order to Attorney General Robert H. Jackson in which President Roosevelt said he agreed with the broad purpose of the Supreme Court decision in *Nardone*, but could not think, and he was of course right, that the court was then considering the risks the country faced from international conflict, and he had to think of the fifth column and the history of Western Europe and the preceding several years. Therefore, where there was substantial risk of international violence, "grave matters involving the defense of the nation," or subversion, he was ordering the use of wiretap. "It is too late to do anything about it after sabotage, assassinations and 'fifth column' activities are completed," he said in his letter of instruction. He said in the last paragraph of his letter that it should be limited to the "minimum" and limited "insofar as possible to aliens."

The scope of the use of electronic surveillance during the war is, I think, probably impossible to recreate, but we got a lot of handy practice at it. But we have some indications of the extent of the FBI use just before December 7, 1941, and they are pretty interesting, too.

For instance, in a period between September 2 and October 2, 1941, just a couple of months before Pearl Harbor, the Federal Bureau of Investigation asked Attorney General Francis Biddle to authorize seven wiretaps. Two were on persons who had some relation to Germany. One was an office, the German commercial attache in New York City. Another was on a German citizen who had an automobile with a shortwave radio in it.

Two had to do with Japanese. One was placed on the Japanese consulate at San Francisco, and the other was to monitor all telephone calls from Hawaii to Japan. That request was made September 2, 1941.

The other three all involved alleged Communists. One was a young woman in San Francisco, one was a man who lived in North Hollywood, California, and the third a book store in Mr. Biddle's town of Philadelphia.

All the wiretaps, except that in the book store in Philadelphia, were authorized. Most requests, however, even in those days were pending for more than a month before they were authorized.

We had wiretaps on the transpacific cables, cables to Hawaii, and were regularly monitoring all electronic communications over them in the months preceding Pearl Harbor. Of course, you are not looking at the foreign affairs area this morning, but if it gave us any warning we didn't act upon it.

In July 1946 Attorney General Tom Clark, consistent, he said in his memo to President Truman,

with the acts of his two immediate predecessors, sought and obtained authority to tap in areas "vital affecting domestic security."

And here is the beginning, at least, of the written record on this problem we have had and a definition of the relationship between foreign and domestic activities, and this also occurred at the beginning of the so-called cold war.

President Eisenhower's first Attorney General, Herbert Brownell, affirmed and expanded that general authority to wiretap in his first year in office.

I think the records of most of these letters are now available. If not, I would urge you to obtain them from the Department of Justice because I think the growth of this is awfully important to look at.

The use of electronic surveillance against organized crime apparently began in the late 1950's while William P. Rogers was Attorney General. I am not aware of any documentary evidence that he knew of or authorized such surveillance. I believe he said publicly he did not.

This activity was expanded in the 1960's and continued until June 30, 1965. Robert Kennedy denied that he authorized or knew of this electronic surveillance. Sometimes there would be as many as 30 bugs or taps in operation in a given city at a particular time. I believe what Robert Kennedy has told us about this. I was in the Department during those years, though not directly involved, consistently anyway, with criminal prosecution.

On June 30, 1965, President Johnson issued his orders drastically curtailing the use of electronic surveillance and requiring that it all be approved by the Attorney General.

I became Acting Attorney General in September 1966, and on the first occasion that I was able to make an accounting as to how many wiretaps were in place, I found 107. I had that reduced, I think, to about 43 by March 27, 1967.

When I was Attorney General, we did not use electronic surveillance in the domestic area, in organized crime. I did have the unpleasant task, following the Fred Black case, of causing the FBI to review all its investigative files in the organized crime area to see whether the Department of Justice had been guilty of using unlawful or tainted evidence in any prosecutions that had gone on before and any investigations or indictments that were then pending. And we voluntarily came into court in scores of cases.

A number of times, embarrassingly, the Supreme Court of the United States confessed there was a possibility of unlawful evidence having been used by the United States Government in cases pending before the court.

To the best of our ability, we sought to determine whether, in fact, any prosecutions from all the bugs of the late '50's and early '60's and the wiretaps, which was primarily the use of bugs, had resulted in a prosecution. And as of the time I left the Department of Justice, January 20, 1969, after an investment of what had to be thousands and thousands of agent hours—it would take virtually four agents to plant a bug the way we were doing it—the FBI contended and I think probably correctly—they also contended its purpose was not to prosecute or send raw data over for prosecution on the basis of information developed by bugs and wiretaps—that none of that evidence had found its way into a single Federal investigation or any state investigation, which makes it a little hard, I think, to explain what it was all about.

Prior to the enactment of Title III, President Johnson sent up his Right to Privacy Act, first in '66 and then in '67—I know I testified in favor of it a couple of times—that would prevent all nonconsensual wiretapping or surveillance in the domestic area.

And sadly, a bill that was to be a right to privacy and had as its hope and expectations the ending of the jungle that existed throughout the United States in public and private unregulated, uncontrolled, and uncontrollable and unlawful wiretapping electronic surveillance, was converted into what is now Title III of the Omnibus Crime Control Act of 1968.

It is interesting to watch the abuses and wonder what they have cost us.

I would ask many times—and I think it's an important question—whether it is possible that the wiretaps on Martin Luther King, Jr., contributed to the demise of the civil rights movement. I believe to some extent, at least, they did, because I can remember the days that Martin Luther King, Jr., was very welcome in the White House, and then for reasons that I didn't understand and still don't know, I can remember when he was no longer welcome there before his death.

It is interesting to watch how an Assistant Attorney General for the Criminal Division, who had engaged so vigorously in the rhetoric about wiretapping, Will Wilson, later asked to resign as Assistant Attorney General in charge of the Criminal Division, it having been disclosed that he, immediately before becoming an Assistant District Attorney, had signed a check—whether or not he knew the purpose was debatable—which was then transmitted to a private investigator who was under indictment for wiretapping a Federal bank examiner. I think that is how it happened.

And once you start down that road, the idea you make fine distinctions is proved wrong by experience. You have violated what I consider to be some fundamental moral principles. You don't respect the integrity of the individual or his privacy, and soon you are wiretapping the press and your own assistants, and finally your own brother.

I would urge you, with all the ardor of which I am able, to end this miserable business. It is unworthy of the country by whose principles we live and are free.

CHAIRMAN ERICKSON: General, regarding Title III, certain areas within that statute might be worthy of consideration as far as the protection of privacy is concerned in suggesting amendments.

As you know, the sale of devices and the manufacture of devices that can be used for electronic surveillance purposes is so rampant now that you can buy devices within a few blocks of the Federal Bureau of Investigation.

Don't you think there should be some effort made by Congress to require that manufacturers be licensed to sell this equipment that can be used for electronic surveillance?

MR. CLARK: I would prefer that they be prohibited. I have seen so much evil that comes from it. We have just finished a four- or five-month trial in Buffalo involving the Attica Prison rebellion, and if we had back the time we spent running down rumors that have never panned out about wiretapping—and literally within the last 30 days in a letter that came to me from the Lawyers Committee for Civil Rights, I was told that by coincidence, in a place along New York Avenue that we all know about, he overheard someone in conversation at the counter there talking about some bugs that had been purchased for use in the investigation—I am not talking about a wiretap; rebellion after all—but in the investigation and prosecution that resulted later in just that sort of thing, in the Berrigan case. And finally after the trial, you find that without a court order the FBI used taps in the course of investigating the case of Berrigan, a professor at Haverford College, and others. I don't think we ought to regulate it. I think we ought to prohibit it.

CHAIRMAN ERICKSON: If the sale of this material is as rampant as you seem to think it is, there should be some effort to control it. Don't you believe that's true?

MR. CLARK: I agree.

CHAIRMAN ERICKSON: And is there any question in your mind that you can buy nearly any type of electronic surveillance gear now?

MR. CLARK: No question in my mind. We could walk 30 minutes from where we are sitting and buy

some pretty sophisticated equipment over the counter, on public sale.

CHAIRMAN ERICKSON: Regarding the procedures that are outlined in Title III, do you think requirement that the Attorney General pass upon each application for electronic surveillance permission is in keeping with the needs for privacy, or could that be delegated to the Deputy Attorney General or somebody else along the line?

MR. CLARK: Well, you are taking me into the nitty-gritty. I am perfectly prepared to go in there. I have to say that I do so still believing that sometime or other we have to muster whatever qualities it takes to say, "We are not going to do this, period."

While we do it, I would seek the most effective and comprehensive types of checks, and I would prefer to see the Attorney General approving them.

CHAIRMAN ERICKSON: Just as the statute is now?

MR. CLARK: As the statute is now, if it has to be done. Because I think the sensitivity to the meaning and the political exposure to the administration, and the care and concern for reputation and other things, will be keener there.

CHAIRMAN ERICKSON: Prior to the enactment of Title III, of course, the primary source of regulation and restriction of the interception of telephone conversations was Section 605 of the Federal Communications Act.

Do you feel that was effective and served as any restriction on the Department of Justice?

MR. CLARK: Well, I think so.

My judgment is that the reason for the extensive use of bugs and the organized crime investigation activities in the late '50's and early '60's was the principle to take care of the Bureau. It was known that if you engaged in wiretapping, some fool Attorney General might prosecute you under 605, but if it were electronic surveillance where no statutory inhibition attached, the worst that can happen to you would be you'd be perhaps embarrassed and perhaps lose your job.

That is an opinion. I believe that. I can't prove it.

CHAIRMAN ERICKSON: Section 605 was intended in the Department to mean "intercept and divulge." And wasn't the interpretation that it was intercepting and not divulging and therefore not within the Act? Wasn't that the general interpretation?

MR. CLARK: That was the interpretation placed on there, and it just shows you that once you break your principle, words will not suffice to protect or safeguard valuable interests that the principle was designed to protect. Because clever people will find constructions of words that will permit them to engage rather freely and extensively in what it is they want to do.

CHAIRMAN ERICKSON: You suggested a violation of Section 605 resulted or could result in the prosecution of individuals who had surveiled with wiretapping.

Do you know of any such prosecutions that ever occurred?

MR. CLARK: Well, unless I am mistaken—you can get this in the records of the Department of Justice—there were a number of prosecutions—not many. They all involved, insofar as I recall, private use.

I know my state of mind as Attorney General, and I think Mr. Hoover knew my state of mind. And that was if I ever learned of an FBI wiretapping where it was not authorized, that I would prosecute him. And I think I must have had some reason to believe I had the power to do that. I am sure it was an almost unenforced statute, and from the great literature in the field we see that there were widespread violations.

CHAIRMAN ERICKSON: As a matter of fact, didn't Mr. Hoover seek appropriations from Congress where there was a question of buying equipment for wiretapping, and it was then justified on the basis that it was to be used to intercept but not divulge? Do you know of that?

MR. CLARK: I think that concept finally obtained—at least the concept of silence from the Congress, from the Executive, and from the courts—some courts anyway.

CHAIRMAN ERICKSON: Now that we have Title III, though, the protective provisions of that act offer more protection to the right of privacy than was ever afforded by Section 605 of the Federal Communications Act. Wouldn't you agree with that?

MR. CLARK: No question in the world about that.

CHAIRMAN ERICKSON: So we have made giant strides forward in protecting privacy by the enactment of the Omnibus Crime Control and Safe Streets Act.

MR. CLARK: Well, in a pragmatic sense, yes. We have also, for the first time, stated as our national principle—and my concept of the utility of law and its capacity is that it is little more than a way of stating your principles and what you stand for and what you are going to try to do.

And for that pragmatic advantage, we paid a heavy price. We said, "This is a dangerous belief, and this we believe, and this we shall do." And we authorized it. And I think that affects people's attitudes towards conduct.

I think it's symbolic. If you can really weigh it out, it's symbolic. And the political argument is just an argument between fear and freedom, and the

meaning of the actual use of electronic surveillance in law enforcement is infinitesimal. It is just not there for measurement purposes.

CHAIRMAN ERICKSON: Do your beliefs go so far as to the fact that there should be a limitation on consensual eavesdropping, if you will?

MR. CLARK: Yes.

CHAIRMAN ERICKSON: Such as the person communicating as they did in the *Osborn* case to preserve the testimony or the conversations that occurred to prevent them from being distorted at the time of trial?

MR. CLARK: The *Osborn* case was a trouble to all of us in the Department at the time. It really was so painful to me that I did not believe I could go forward under the circumstances with the prosecutions and so recommended, although I don't know of anything I find more corrupting of our total system than fooling around with a jury.

CHAIRMAN ERICKSON: But these consensual eavesdropping experiences placed in granite a conversation that occurred and eliminated the need for two people to give their own personalized view of what they said.

Don't you feel that tends to make the search for truth more meaningful?

MR. CLARK: Well, I think your parameters are too narrow. Its use affects our total relationships in many ways, and the granite that you referred to may be a pretty small rock compared with what would otherwise be a freer and more trusting relationship.

It is said if there is anything we should learn from the whole Watergate phenomenon, it is our failure as a society that proclaims the rule of law as its governing force to face up to the total variety of investigative practices and techniques, and make the hard decisions for the man in the street, the officer who has to decide now what to do.

You know, I watched the use of consensu-als. It is hard to find time to think as Attorney General, and I was focusing on wiretapping and bugging, but I took it that I had the power to advise all the Cabinet officers and agency heads that consensual devices would also require my approval as Attorney General.

I didn't hear any objection—I did hear objection but I didn't hear any refusals from them, and I assume it began to be done. The people who protested most of all were the Federal Bureau of Narcotics, Secret Service, and a couple of others.

It was very interesting to watch how they'd go about it. One thing they claimed is that emergency situations arise when it is impossible to get hold of the Attorney General. You have to send an agent into a meeting right now, and he is going to lose his

life if he doesn't have a transmitter with him. That's the psychology of it.

And watching the use—there is a record of it in the Department of Justice—the use immediately went way down, and all those emergencies that everybody foresaw, you know, where someone is smuggling a nuclear bomb over Manhattan, and it is going to go off unless you can find out through a wiretap where it is, never occurred.

CHAIRMAN ERICKSON: In dealing with the Knapp Commission, you mentioned the thing that helped the most was an honest cop.

MR. CLARK: Yes.

CHAIRMAN ERICKSON: The honest cop is, of course, the key to any such investigation. But the statements of that honest cop are best verified if that conversation that he has had with the dishonest cop can be duplicated by way of an electronic report.

Isn't that correct?

MR. CLARK: Well, if he doesn't think so now—speaking of Frank Serpico, whose story I believe to be one of the most important that this country should know—I am not talking about the movie or the book, which I am not too keen on—he shows for the honest one it is very difficult. And for most people engaged in rough-and-tumble activity today, it is hard to know what you are doing. But on reflection, I think Frank Serpico agrees that this is not the way to do it. And we find the dishonest cops are the ones who are managing the taps.

CHAIRMAN ERICKSON: In connection with his activities, he used a body recorder, did he not?

MR. CLARK: That is right.

CHAIRMAN ERICKSON: As to the Title III provisions relating to emergency taps which permit surveillance, do you feel that that provision in Title III would pass constitutional muster?

MR. CLARK: Well, I would like to see the day where there is the full Fourth Amendment analogy to electronic surveillance.

And I guess I think if that were the case, the probability of constitutionally permissible instances arising would be decades apart. You know, you can investigate crime in many ways, and chance will stumble towards you once in awhile. But I just don't believe that that is a scheme that was seriously intended. I think it appeals to fear and conjures up the idea that there are these very great dangers, and unless we are tough enough and stern enough to meet them, we will be undone. And in fact, the great probability is of our being undone by succumbing to that type of reasoning.

CHAIRMAN ERICKSON: Well, at the time our Commission commenced its work, we learned that the Department of Justice has not used the emergency provisions since the enactment of Title III.

MR. CLARK: They haven't in a decade yet—once in a decade, maybe.

CHAIRMAN ERICKSON: Do you feel that provision is constitutional?

MR. CLARK: I would hope not. As I say, I can conceive what I would consider a constitutional application, but it would have to conform with the full body of Fourth Amendment law as applied to electronic—and that is not an easy intellectual exercise—as applied to the electronic phenomena.

But I think the probability of that case arising is almost nil, and that means that that provision would fail, at least in its application, in nearly all instances.

CHAIRMAN ERICKSON: In dealing with national security and electronic surveillance, that was excepted from the provisions of Title III, where the President can act to protect national security.

Do you feel that there should be any change in Title III relating to that area of surveillance?

MR. CLARK: Well, I sure do. The history of the exemption, as we now call it, is very interesting. It came straight out of the FBI. It is the only provision when the bills were going up initially, at least, that did.

You know, it protects big business, a big operation in the national security field—not protecting us from any threat of violence, but just the power of knowledge.

I have testified at length in the past about requests for authorization that I turned down. You'd find a foreign group would be coming to this country to negotiate a treaty, and you could find the individual who is engaged for the United States in negotiating that treaty and say, "Let's wiretap them, and then we will be the best negotiators you ever saw."

That is the sort of thing that it leads to.

If you really want to try a difficult, but very important investigation, study the politics of this. You will be able to find that most of the national security taps that I authorized were absolutely unnecessary and wasteful, and that everyone conceded it, and to manipulate the total figures later—because these were all on embassies, up and down Massachusetts Avenue, and things like that. And you know you get every imaginable kind of conversation on them, and you really don't get a body of knowledge that tells you their interests and habits and nominal interest at the moment.

But the national security is served. And they realized it when they began to play the numbers game. And the numbers game in electronic surveillance and wiretapping is a very real game. So they'd take them off the Ecuador and all these other little countries and use them where they wanted to because they were never there anyway.

I pulled them down from over 150 to no more than 100. That was the best I could do at that time. I think they were terribly wasteful. I believe in this country and its principles and I'd like to look at a foreign official in the eye and say, "No wiretapping. I don't think it's good and I don't think it's necessary."

And as I pointed out earlier, it didn't help us at Pearl Harbor.

CHAIRMAN ERICKSON: Thank you very much, General.

Professor Blakey.

MR. BLAKEY: Mr. Clark, I'd like to welcome you to this Commission. I am an admirer of your courage and forthrightness in this area. You certainly had the courage to say things that other people didn't have the courage to say—to swim upstream when all the other fish were going the other way.

I welcome your testimony, and I wonder if I could ask you one or two preliminary questions.

You said when you were Attorney General that you did authorize some electronic surveillance in the security area. You did not authorize any domestic security cases; is that correct?

MR. CLARK: That is correct.

MR. BLAKEY: How would you classify the Communist Party?

MR. CLARK: The Communist Party would not fall "either/or." For instance, I turned down requests on agricultural attachés in Communist embassies themselves. Because agriculture—? I didn't see it.

The Communist Party publications and things like that were sometimes turned down—things in that area. On the other hand, sometimes a trade company which sounds innocent enough would be authorized. But underlying that would be an allegation that they were engaged in activity directly related to military security from the standpoint of obtaining secret technology or threatening sabotage.

MR. BLAKEY: Was that the only area where you authorized surveillance of Communist Party personnel?

MR. CLARK I tried to formulate a standard, and if it could be expressed in words—I think that we will probably find the words back there. We'd say, "Where there is a clear, substantial, immediate threat to the military security of the nation?"

Now, sometimes this would involve people at the scene of the Embassy, just looking at their credentials. But you'd find out that they were trying to gather up plutonium—I say "find out"—you were told they were trying to gather up plutonium or something like that. I don't know if they were or not.

Virtually all cases were made.

MR. BLAKEY: For aliens, was that the principle you applied?

MR. CLARK: Alien citizenship?

MR. BLAKEY: No, security.

MR. CLARK: Security.

MR. BLAKEY: Did you ever authorize any surveillance of Communists who were not Soviet citizens?

MR. CLARK: I am not sure. I think maybe that didn't come up, or if it did, not very often. And the reason was that the days of the Security Board were pretty much over, and the Bureau engaged in just enormous bugging of not just the Communist Party, U.S.A., but any group that you could think of that might have the wildest association with CPUSA.

I opposed the Subversive Activities Control Board and said I would not send any cases up that were tainted by unlawful evidence. In other words, I would treat that Board—a lot of people thought it was a trick, and I have never exactly known what it was.

MR. BLAKEY: It got rid of nearly all the cases before the Board.

MR. CLARK: Yes, but it had this sad result. You'd pick up a teacher in Salt Lake City. You'd pick up a guy with cancer.

Having said that, I think there may have been some continuing taps on the Communist Party, U.S.A., and if so, they would be supported by requests that would say they were acting as agents for foreign nations and seeking to do these various things.

MR. BLAKEY: What I want to explore a little bit with you goes like this: The rationale I heard for the King tap, absurd as it might seem, was that a staff member was Communist influenced, and the effort, however benign in intent, was to attempt to insulate him from improper Communist influence.

This was before your tenure, and I certainly don't want to associate you with it. I was wondering if that was the sort of test you applied when you said national security?

MR. CLARK: No, the King taps were put on in October 1963. The Attorney General under President Kennedy—to reiterate the importance of it, and what you might call roughly the subversion of the civil rights movement—whether that was the controlling factor or not I don't know. He did authorize them.

After he left office there were some bugs placed on Dr. King.

In contrast, the FBI was still seeking to tap and bug Dr. King when I was Attorney General, and I turned them down three or four times. It always puzzled me that they kept coming back on that one because usually when I say “no,” that's the end of

it. But as late as October 1968, they came back and asked again.

I don't know if that is a rationalization for the reason. To me it would be adequate.

MR. BLAKEY: I'm trying to figure out what types of problems are included in the national security category, what you did include in it, and what you didn't. Apparently, everybody puts different things in it.

MR. CLARK: I had a theoretical distinction. You understand I opposed the national security tap, too. The theoretical distinction to me was this, that the country under a constitution such as ours should be able to control any social conduct within its borders by fair means. I believe that. I do not believe wiretap is a fair means.

On the other hand, you can't control conduct outside your borders, and it can hurt you. And you can cite Cuba, troop movements in Eastern Europe, something like that. The need to know can be quite important. And, therefore, you have that theoretical distinction. I don't accept it, but I think it's valid in terms of political science.

MR. BLAKEY: Just as another example, would you have ever authorized surveillance on, say, Gus Hall?

MR. CLARK: I don't think it ever came up. I have no recollection of it.

MR. BLAKEY: Would, say, a routine meeting by him and one other member of the Communist Party have been the kind of thing that you would have authorized surveillance on?

MR. CLARK: You know, I don't engage in hypotheticals contrary to fact. I just think it is the effect of George Santayana on me. It is not logically permissible. You have to deal with practicality. Each authorization request was practicality. I don't recall any time when any request ever came in that had to do with the Communist Party holding any particular meeting or anything like that.

MR. BLAKEY: Is that the kind of thing that would stick in your mind?

MR. CLARK: Oh, sure, I would think so. I think that was past. I think that was an interest in the late '40's and '50's.

To the extent that we had any on Communist Party activities, they were more or less permanent and more or less simple.

MR. BLAKEY: Would you be surprised if one turned up?

MR. CLARK: My view has always been that Mr. Hoover did not authorize taps or bugs that I did not approve. And he didn't encourage what we used to call suicide taps or bugs, not authorized ones where the agent bears the responsibility.

So I don't think—and I have not yet been shown—a bug or a tap while I was Attorney General was placed in violation of President Johnson's orders.

So I think you'd find that any that were on there were ones that I authorized.

MR. BLAKEY: I didn't really come away with a firm impression of your attitude towards consensuals insofar as they might be based on court orders. Would you support them based on court orders?

MR. CLARK: I would certainly require, as a matter of policy, a court order. I think I would prefer their prohibition. I don't think we really need them. I don't think the idea that there is a specificity or factuality that comes out of them that is that helpful.

MR. BLAKEY: I think it really is unfair if you are against something to ask you how you'd set the system up.

MR. CLARK: How I set it up?

MR. BLAKEY: Yes, how would you set it up. I don't think it's fair for me to ask you what kind of system you'd set up under a court system. That is what I was going to explore with you, but if you are against it, there is no reason why you should be asked to take positions on the details of it.

MR. CLARK: We do that in life all the time, but I appreciate your effort.

MR. BLAKEY: Professor Schwartz will be able to discuss it.

MR. CLARK: He'd be pretty good at that.

MR. BLAKEY: Let me turn to another area. You were quoted—and I suspect unfairly—this is way back, in 1967, in an interview by Sidney Zion on May 19, 1967—

MR. CLARK: He interviewed me on the 17th. I had gone up to New York for the anniversary of *Brown v. Board of Education*. And he rode back with me in a cab from the airport.

MR. BLAKEY: He said you considered organized crime "a tiny part" of the entire crime picture. Is that accurate?

MR. CLARK: You will find in the *Congressional Record* a series of letters, as I recall, between Chairman Emmanuel Celler and myself. It's been a long time ago. My recollection is the substance of it was that I had no recollection of the conversation. I knew Sidney Zion and remember that he asked whether he could ride out in the cab. I was for civil rights. That is what I had been up there for, and that is what we talked about.

I do believe—and I have tried to express it in various places—that we exaggerate the role and nature of organized crime, to our great injury. It is serious, must be eliminated. I think wiretap is essentially irrelevant to it, as I have suggested.

It is so anomalous to me that since Title III you have had from 55 to 80 percent of the bugs by state agencies in New Jersey and New York every year—more than half in those two states. Most states never use it.

MR. BLAKEY: It is a fact that most of the other major metropolitan areas that have organized crime—Michigan, Ohio, California—have not adopted statutes, so there is no way they could very well use them.

The states that have adopted them, I think it's probably fair to say a number of them, don't have an organized crime problem, and sometimes you wonder why they adopted it if they don't have organized crime.

MR. CLARK: Well, it is a very sad experience to watch a state legislature—I have done it through the states and in some foreign countries, testifying, too—tortured with what I consider to be the demagoguery of the fear of crime, over whether to vote for or against wiretap authorization in a little old rural state that has got no more use for it than it does a subway system.

MR. BLAKEY: There is clearly a lot of political demagoguery—

MR. CLARK: On both sides, perhaps, but it is such an irrelevant thing. I think I recall Colorado, when I was out there once, and Oregon recently, tortured by the legislative debate. And it is something that really concerns legislators from the standpoint of their vulnerability at the polls next time.

MR. BLAKEY: Let me go back to—as I said to begin with, I don't want to stick you with Sidney Zion's label. But I would like to explore with you in the context of a public hearing what you feel the impact of organized crime is in our society. And let me make clear for you the context in which I do this.

One, the issue raised before the Commission is not only the effectiveness of wiretapping, but even assuming it is effective, whether it would be worthwhile at all. A good deal of this discussion has centered on, for example, gambling prosecutions. "Sure, it is effective, but after you've done it, so what?"

And particularly in your case, some of what you have said has been quoted and used by people in wiretapping arguments to say that organized crime is not really a serious problem.

MR. CLARK: It is a tiny part of the entire picture.

[Inaudible.]

MR. BLAKEY: So what I'd like to hear from you is your assessment of organized crime in the United States and how important is it to us to do something about it in its various manifestations.

MR. CLARK: I'd like to eliminate it. I'd like to win. You can really win that one, you know. You can really win. I can't think of anything I'd enjoy much more than organizing or helping organize the first Strike Forces. I announced them before I became Attorney General, really, Acting Attorney General. We were really going to be gangbusters.

I think the concept was solid and had it been followed faithfully I think it could have liberated many localities.

But I am concerned with crime. I think violence is the ultimate human degradation. I look at hundreds and hundreds of violent crimes throughout the country over the years, and the chance of wiretapping touching one in 10,000 is very small.

There are three qualities that will always be essential for the existence of organized crime. We have to remember there are whole nations free of it; there are whole states in this country that are free of it. You have your burglary crimes and car theft rings and stuff like that, but not organized crime.

You have to have millions of people, because organized crime is doing a daily trade. It is a lot easier to find out where its services are than the wiretap business we were talking about earlier because it is a bigger business and they are out on the streets looking for you, and you and I can go to any town in the country and find out where the gambling is and the narcotics and the prostitution and the high-rate money, if we just got a little savvy.

But it's a real power base and it preys on weak people, because it has to be there every day. And if people have power they can say, "Look, I'm tired of this. I am through with it. I can talk to the mayor; I can talk to the chief of police, I can talk to the DA and get some response."

It is enormous hypocrisy in law to say police have power to do certain things they don't have the power to do. It is hopeless to send them our enforcing laws that can't be enforced in that way. Gambling used to be 75 per cent of the take of organized crime—billions of dollars. And you just can't police it away.

And the idea of talking about the politics of the numbers and wiretap—you'd see Attorney General John Mitchell saying on his wiretaps, "We got hundreds and hundreds of incriminating wiretaps." Of course they did. It was a bookie joint. Why did you need a wiretap? You could bust it in other ways. You are playing politics, and I said so at the time.

With narcotics the same way. You can't beat heroin out of the budget of an addict. It is a very complex social medical problem. To try to legislate it away is a mistake. Then to try to give law enforcement wiretap and other means to enforce it

away when it is something that can't be done that way is wrong.

So you have to decriminalize. You can't make the world safe for hypocrisy. Your laws have to be honest and susceptible to enforcement.

Second, you have to have corruption for organized crime. It is impossible to have organized crime without corruption. We knew that in '31 with the crime report from Wickersham, and we knew it in '67 with the crime report from Katzenbach. You don't even have to think to know it. Because you can find it; it's there; everybody knows about it. Critical areas are going to be corrupted because it can't exist without that.

And, therefore, I think we can wipe organized crime out. I think we ought to. But I think we may get the central focus of a phenomenon we call crime in America, but to assume that by ridding the country of them "we will live happily ever after" is wrong. Because you look at the crime rates in the cities and areas that don't have organized crime, and they are not perceptibly different as far as you can tell. I don't really believe in the statistics of the places that have organized crime.

So I say do it. You can get rid of it. It is a joyous fight, and I am on the side of the angels, but do not consider it to be the heart of the problem of crime in America.

MR. BLAKEY: Dr. Martin Luther King in November of 1965 wrote in the *Saturday Review*, "The most grievous charge against the municipal police is not brutality, though it persists. Permissive crime in the ghettos is. Permissive crime is the name of organized crime in the ghetto, designed and operated by the crime syndicates, selling narcotics freely in the protective sanctuaries of the ghetto because no one, including the police, cares particularly about ghetto crime. It pervades every area of life."

Would you associate yourself with that statement?

MR. CLARK: I think Dr. King is one of the greatest people that ever lived. I watched black civil rights leadership go through that phase. I watched Whitney Young, Jr., who was on the Crime Commission vote for wiretap. And the reason was he felt so strongly that the victims of organized crime—and God knows he was right—were the people he was trying to help.

I never had a conversation with Martin Luther King, Jr., and if anyone knew how it felt to be victimized by wiretap, Martin Luther King would. But I worked with Whitney Young before I left the Department, and he came to oppose wiretapping because he came to see it could do enormous harm and not liberate his people from organized crime or liberate so many people who are held captive there.

MR. BLAKEY: When you suggested one of the causes of organized crime was the law itself and its over-criminalization, would you suggest we decriminalize narcotics possession and use—not marijuana—but cocaine and heroin?

MR. CLARK: Those are complex subjects. I basically feel that to apply the criminal sanction—it has turned out civil commitment was nothing but a new jail with the same bars and same guards, and so forth.

MR. BLAKEY: The federal program was never really financed.

MR. CLARK: That is right. It's like all these things. You know, we make the gesture and that is how principles get destroyed. We never really do what has to be done to live up to the principle.

MR. BLAKEY: Would you suggest that in our society that we could maintain our love of human dignity, our civilization, and give away narcotics?

MR. CLARK: I have always opposed maintenance programs. I say that painfully.

MR. BLAKEY: How then would we decriminalize cocaine or heroin possession?

MR. CLARK: It is hard to put in a nutshell. Basically, the idea that you can treat meaningfully the phenomenon of addiction by imprisonment is false and dangerous. We have more addicts walk out of prison than walk in.

MR. BLAKEY: No, it is—

MR. CLARK: I think what you have to do is address your laws at people who manufacture and transport and wholesale them. I think you need to attack at those critical points as effectively as you can.

When you come to the addict, I think what you have to do is to give them, in addition to the other citizens of our slums who are the ones who suffer from this, rights to health finally. And that means you have got to invest in the things—for instance, I think if we took a third of the energy that has been spent on wiretap debate, which has not helped or harmed law enforcement in my judgment, and put it into chemical laboratories, we'd find a chemical substitute to relieve the body of the desire for opium and its derivatives. That has never been done.

People have rights to health. If we realize you can't cram health down anybody's throat, we could arrest the problem easily.

If there is any single area of enforcement that the Nixon Administration consistently highlighted, it's what they were going to do with drugs. And in my judgment, it's a bigger mess now than it was before they began. As a matter of fact, I read something about that on the front page of the *New York Times* today. And that is because they started with the

wrong premise, that you can beat people around to do things your way. It doesn't work.

MR. BLAKEY: Do I understand what you are saying is perhaps some sort of decriminalization of addict possession might be viable, but as to importation, sale, and distribution it would make sense to keep the criminal law?

MR. CLARK: Yes. I realize that creates some dilemmas, but there are dilemmas in life, I guess.

MR. BLAKEY: I take it most of the people who have argued for wiretapping have not argued for it as a means of catching addicts, but wholesalers and importers and distributors.

MR. CLARK: But look who they catch.

MR. BLAKEY: You made a statement that I was much attracted to earlier about the symbolic importance of the law. I wonder if I could quote you again a short passage from an essay by Thrasher on *The Gang* talking about what the impact of the law is on young people in the ghetto and ask you to comment on it.

"When a noted criminal is caught, the fact is the principal topic of conversation among boys. They and others lay wagers on how long it will be before the criminal is free again, how long it will be before his pull gets him away from the law. The youngsters soon learn who are the politicians who can be depended upon to get offenders out of trouble, who are the dive-keepers who are protected. The increasing contempt for the law is due to the corrupt alliance between crime and politics, protected vice, pull in the administration of justice, unemployment, and the general soreness against the world produced by these conditions."

Would you agree that that kind of statement is probably accurate as to what goes on today?

MR. CLARK: Well, I think that that is a fact. My experience with youth crimes and gangs and all that is that maybe 10 per cent feel that phenomenon very strongly. But the great majority are oblivious to all that sort of thing. They are just kind of running with the crowd, you know—what else is there to do? So it is an exaggeration. It is an overstatement. The idea that that is a conscious awareness of the majority of youngsters living in high-crime areas with gang activities is contrary to my experience.

MR. BLAKEY: In light of your answer, let me read you another short passage from the Riot Commission. Again I quote:

"With the father absent and the mother working, many ghetto children spend the bulk of their time on the streets—the streets of a crime-ridden, violence-prone and poverty-stricken world. The image of success in this world is not that of the 'solid citizen', a responsible husband and father, but

rather that of a 'hustler', who takes care of himself by exploiting others. The dope seller and the numbers runner are the 'successful' men because their earnings far outstrip those men who try to climb the economic ladder in honest ways.

"Young people in the ghetto are acutely conscious of a system which appears to offer rewards to those who illegally exploit others and failure to those who struggle under traditional responsibilities. Under these circumstances, many adopt exploitation and the 'hustle' as a way of life, disclaiming both work and marriage in favor of temporary liaisons. This pattern reinforces itself from one generation to the next, creating a counter-culture of poverty and ingrained cynicism about society and its institutions."

Would you say that, too, is an exaggeration?

MR. CLARK: I think that, too, is a fact. I think to apply it generally is untrue and unfair. I do think it's a psychological phenomenon of greater pervasiveness than the earlier one, Thrasher.

The reason is basically there is more contact and experience between ghetto youth and hustlers than the other. That tends to be hearsay, the politics and corruption at that level. They don't see that directly. The other they see directly. They know who is wearing good clothes and has the car, and they know who is making out.

But to say that characterization is accurate as to even the great majority of kids in high-crime areas—and I'm talking about all the kids, the ones who are really dropping out of schools, and from broken families—is probably an exaggeration. It is a real phenomenon, something to worry about, but it's not universal.

MR. BLAKEY: The issue is the attempt is sometimes made to evaluate organized crime by head count, "How many Mafiosi did you catch and how many indictments did you get?"

I am really trying to ask you if this kind of program through its successes—using whatever means, Strike Forces as opposed to wiretapping, or wiretapping—and its failures, might not have a broader symbolic impact in the community, that is, do you think that the failure of our society to apprehend, convict, and sanction people who can in the community be seen as leaders of criminal groups has an impact widely on other people and their allegiance to the law?

MR. CLARK: The idea that you can create some higher level of respect for law by more systematically picking off the hot shot, so to speak, in the ghetto, is wrong. The problem is it will do just the opposite.

First, it will involve you in almost war.

Second, as soon as you do it, you are attacking almost all the leadership there. It's almost the same thing as you see in South Africa—you pick off all the leadership. Whenever anybody sticks up his head, you pick off the leaders because you want the rest to remember him martyred.

MR. BLAKEY: I heard a number of persons express anyway, when Jimmy Hoffa was convicted, particularly for jury bribery, that this was an important statement about the rule of law, and he was not above the law. And conversely, a lot of people said when the former President departed, this was an unfortunate act, that it undermined the rule of law, because somehow it said if you get to be President you get a license.

What I am kind of raising with you is: If there are people known to be criminals, exploiters of their fellow citizens, does our society by allowing these people—I am not raising the question of wiretapping with you—to go free of sanction have a wider impact than simply permitting them to continue their activities?

MR. CLARK: The crime is not letting them go, but permitting the living conditions that prevail, the unsafe housing and disease and sickness.

MR. BLAKEY: Do we have to choose? I mean, if I sort—

MR. CLARK: The idea that the kids that used to run the gangs, the slum being exactly what it was before, will now respect the law is wrong.

CHAIRMAN ERICKSON: I wonder if this would be a good time to take a recess.

If it is agreeable, we will recess at this time until 1:20, and we are to reconvene in Room 4200. And you should take your materials with you since there will be another hearing in here at 1:00 o'clock.

[Whereupon at 12:30 p.m., a luncheon recess was taken until 1:20 p.m.]

AFTERNOON SESSION

CHAIRMAN ERICKSON: General Clark, one thing we try to do in this Commission is to remain on time, and I hope that our questioners will remember that as well.

So with that short preamble, the meeting is reconvened.

Professor Blakey.

MR. BLAKEY: Attorney General Clark, we were discussing, I suppose, what is a kind of perennial problem in so much of this, the problem of choice. And let me see if I can't rephrase and put in a broader context the type of question I asked you.

Running through a great deal of what you said today in answer to my specific questions is a kind of dichotomy. I don't necessarily associate you or myself with it; I present it as a general position.

One person says "law enforcement" and one person says "socioeconomic conditions."

If one says, "Let's fight narcotics with criminal sanctions," someone else says, "No, let's not handle it that way; let's handle it with civil commitment or chemical agents to treat addiction."

If someone says, "Let's fight organized crime," someone else says, "That's not the big problem; let's do the big problem, which is street crime," which is the violence in the street, the rape, robbery, the inability to walk in the park at night.

My question for you is: Is this one of those social situations where we do face a hard choice? Can't we have both? That is, can't I be for ameliorating the economic and social conditions in the ghetto and also—and I am not talking about wiretapping—be for crime control? Can't I be for treating an addict as a human being and at the same time be for using law enforcement techniques to fight crime by whatever means, even if it is a bare minimum of seeking incapacitation as a means to deal with people who ply the drug trade?

Do I really have to choose? Can't I fight organized crime and street crime? And let's throw in a white collar crime, price-fixing or tax evasion, too.

Do we really have to choose in these areas?

MR. CLARK: No, I don't think so. I would certainly consider myself as favoring effective and efficient enforcement of laws against all forms of antisocial conduct, whether it's things that are stolen through white collar crime or the muggers, or the organized crime payroll.

But I think the real question as to wiretapping is whether you can permit techniques of enforcement that are inherently unfair or immoral.

I won't make the value judgment, but assuming that they are so to a degree—

MR. BLAKEY: The rack and the screw. We just don't torture people any more.

MR. CLARK: I hope not.

MR. BLAKEY: And if we do, no one in our society argues that a court-ordered system should permit it. That is just beyond the pale.

MR. CLARK: I hope so. But I think the imperative need is that we have the courage to say that we will act fairly in the enforcement of our laws, and then start that process of determining what we consider acceptable by that sort of approach.

And doing that, I first, at a moral level, find wiretapping unacceptable.

And finally, it seems to me, although there are a series of other objections, that it is debilitating and corrupting itself, because it, too, demeans the dignity of all involved, including the poor agent that is sitting there with the headphones waiting for somebody to say something they should never say.

MR. BLAKEY: But I take it it is your testimony that we don't have to choose; we can fight street crime and organized crime.

MR. CLARK: Oh, absolutely, we must.

MR. BLAKEY: We can deal sympathetically and humanely with the narcotics addict and still be, to use a popular phrase, hard on crime, hard on the pusher, the importer, the one who exploits the individual.

MR. CLARK: You know, if it implies bully force, then it's a declaration of war, and I don't believe in war.

MR. BLAKEY: Certainly not against our own citizens. If we must have military and police, let's have them be constables, citizens on duty.

Assuming we have adequately explored together those kinds of broad general problems, let me return to poor Mr. Sidney Zion's article of May 19, 1967.

You were also quoted in that article on another issue, not really on a value issue.

If one decides that it is immoral, one just doesn't do it even if it works. We don't obstruct justice to elect a President, not because it doesn't work, but because it is immoral; it is wrong. And there is no debate. One just doesn't do the wrong thing.

When I began our discussion, I said that I really had a deep and abiding admiration for the role you have played in doing what I find very difficult, that is, to take a moral position as opposed to a pragmatic or legal or even constitutional position.

For those who say that wiretapping is bad because it's immoral, and reflect a deep conviction, frankly although I do not associate myself with it, I don't have anything but admiration for them and that personal value judgment.

There is a different issue, though, that I think this Commission has to face, and that is a functional question, although it is a very complicated functional question, and that is, does it work? Because, however important organized crime is, however evil, neutral, or good wiretapping is, it is a silly thing to do if it doesn't work.

Let's just reason together a moment about that very difficult question.

You were quoted by Mr. Zion as saying, "With rare exceptions, Mr. Clark said, we have found that electronic surveillance was unnecessary, either in obtaining direct evidence of crime or in developing leads."

Is that an accurate quotation, and does it reflect your understanding of the process?

MR. CLARK: I don't mean to quibble. I don't think it's an accurate quotation, but it states my opinion. I don't recall that conversation with Mr. Zion, but my experience with wiretapping has been

that it is incredibly inefficient. We had a survey made—do you recall Carey Parker?

MR. BLAKEY: Very well.

MR. CLARK: Carey reviewed the logs. He reviewed 13, as I have seen, transcriptions—

MR. BLAKEY: I think it was 12.

MR. CLARK: Was it 12? It was bugs. You may know more about it than I do. The average length was probably longer than 18 months' duration. And a good many, at least a third, during that whole time, a couple of years, disclosed no evidence of any criminal act or any lead.

Well, that is a lot—I think the Peter Balistieri case, Balistieri was allegedly a member of the Mafia in Milwaukee, and the case was transferred to the Southern District of Illinois for trial, as I recall. And there we found what I would call law enforcement gone wild. It is in the record, but just to give you the flavor of it, as I can recall it now, first the bug was discovered because a lawyer that previously had been a candidate for Governor of the State of Wisconsin—I don't remember what his name was; I don't think he was a major contender—had his office remodeled, and behind some wooden paneling I think they found the bug.

From that they discovered that he had been bugged, that a woman named Jenny Alioto, who was a good friend of his as well as his secretary who kept files in her apartment, had been bugged, and Balistieri had been bugged—months and months of this.

Internal Revenue or some other investigative agency, Intelligence, had sought and been denied a search warrant for the Alioto apartment. The Bureau decided to bug it. And, of course, they had to break and enter to get in. And while they were in there—we were never able to establish this, but the probability is they removed intelligence—they looked over there and saw a file cabinet and decided they'd take some of the files out and examine them, and as I recall, photostat them.

My recollection is that nothing was picked up on the bug—at least that was the best that could be discovered—except one conversation with a lawyer in which some young woman whom he didn't know called him and asked him if he knew where she could get an illegal abortion.

It was terribly inefficient.

CHAIRMAN ERICKSON: Before we go further, let me ask one question. As I understand it, General Clark, you have some logistic problem the Commission would like to honor. What is your availability?

MR. CLARK: If I could leave at a quarter of three it would be very helpful. I have a meeting set up for 3:00. If I could leave by that time, it would be very helpful.

CHAIRMAN ERICKSON: Keep that in mind, Professor.

MR. BLAKEY: There are other people who have to come after me.

MR. CLARK: I will try to keep the answers short.

MR. BLAKEY: You said 12 or 13.

MR. CLARK: I said 13, and you said 12.

MR. BLAKEY: I believe the correct figure is 12.

Let me back up from that. Did you have experience as a prosecutor before you came in the Department of Justice?

MR. CLARK: No.

MR. BLAKEY: While you were in the Department of Justice did you ever try any cases?

MR. CLARK: I never prosecuted a criminal case in the courtroom while I was in the Department of Justice.

MR. BLAKEY: I take it that means that you have never actually handled wiretap evidence from a court-ordered system in court or in the Department of Justice?

MR. CLARK: Well, if you want to know whether I have ever prosecuted at courtroom level, the answer is I never have. On the other hand, just from the standpoint of the evidentiary qualities of wiretap, I would say that the surveys that were made were made under my direction. Thurgood Marshall, Fred Vinson were the members—and you had occasion to go through more than they went through. And while I didn't go through it personally I was kept, by regular meetings, constantly advised of it. And it is rather remarkable that from all those hundreds and hundreds of utilizations—I don't say that this is the situation that you have in Newark or the Bronx. It is a different sort of phenomenon. It was not used in prosecutions or leads from which things were used in actual prosecution.

MR. BLAKEY: Of course, they couldn't have been used in court. They were placed in violation of the Fourth Amendment.

It couldn't have been productive in light of the Fourth Amendment.

MR. CLARK: But you are assuming observance of the Fourth Amendment, and you are forgetting bugs were placed in a lawless fashion throughout the country.

MR. BLAKEY: Mr. Clark, I am raising with you—without trying to reanalyze to see whether that surveillance could be done now under Title III, which is a long and complicated legal question—is: What is the experiential base on which you say they are nonproductive?

And I take it it is your testimony that you reviewed the illegal surveillance in the period from the late 1950's through July of '65, when it was shut off, and it is your judgment that that surveillance was unproductive.

Is that correct?

MR. CLARK: Yes, that is part of it.

MR. BLAKEY: And you so testified in 1967 before the Celler Committee:

"We have looked at hundreds and hundreds of bug and wiretap logs, and I think we have experience on which to base a judgment now that we did not have earlier."

You are testifying now, too, along the same lines. You looked at the logs.

MR. CLARK: Yes. In addition, I went through the whole approval procedure and had constant reporting back on various national security taps and was constantly impressed with how unproductive they were.

MR. BLAKEY: You also testified before the Canadian Parliament, I believe, on July 5, 1973:

"The idea that wiretapping is effective against organized crime is wrong-headed in my judgment.

"I had an examination made of 12 bugs that had been installed on alleged members of organized crime. They were in place an average of two years each and grown men, agents of the police, supposedly agents of the FBI, sat seven days a week, 365 to 366 days a year, waiting for someone to say something they should not say."

That is again a reference to the Carey Parker study; is that correct?

MR. CLARK: That sounds like it.

MR. BLAKEY: I wrote the Department of Justice and asked them to make available to the Commission Carey Parker's study in order that we could evaluate the experiential base you offered in a number of public forums as your factual basis that it is unproductive. Mr. Chairman, I would ask that the answer to that letter be incorporated into the record at this point, with my original letter to the Department, so that the readers of the record can see what I am referring to.

CHAIRMAN ERICKSON: It will be so recorded.

[The material referred to appears in the Sept. 16, 1974 transcript.]

MR. BLAKEY: There were, in fact, 12 bugs.

MR. CLARK: That is 12 out of hundreds I screened to be reviewed. But those were in depth. He just sat down and went through them, as I recall.

MR. BLAKEY: But when I go down the 12, I see that the lawyers who evaluated them said that only five of the 12 were evaluated as "unproductive." The other seven were evaluated—and the reason I am reading the ones evaluated as "productive" differently, is that the unproductive ones simply say "unproductive."

MR. CLARK: That means "nothing," then.

MR. BLAKEY: Roughly nothing?

MR. CLARK: No, it means "nothing."

MR. BLAKEY: The first is "unproductive."

The second—and incidentally, there is no indication in this who the people were. At my suggestion, the Department of Justice eliminated the names so we don't know who these people were.

MR. CLARK: They were nearly all in what the Bureau at that time called Cosa Nostra.

MR. BLAKEY: The second one says, "The most productive intelligence source that I have encountered in six years of field experience in crime and racketeering cases."

The lawyer's judgment in that case is that it was productive.

No. 3: "Unproductive."

No. 4: "Very productive. Indicated evidence of murder, loansharking, extortion, gambling, bookmaking, numbers, graft, bribery—magistrate, mayor—perjury, tax evasion, armed robbery."

No. 5: "Moderately productive. Large-scale bookmaking."

No. 6: "Moderately productive. Bribery tax evasion."

No. 7: "Unproductive."

But that meant unproductive to federal agents. They found evidence of state gambling.

No. 8: "Unproductive."

No. 9: "Very productive. Bankruptcy, fraud, bank fraud, narcotics, prostitution, loansharking, corruption of congressmen, undercover payments."

No. 10: "Moderately productive. Official corruption. Bribes of judges and jurors."

No. 11: "Very productive. Bankruptcy fraud; stock fraud."

No. 12: "Unproductive. Some talk of explosives."

I might add here that I have been told that some of the ones that were unproductive were so indicated as being unproductive because the language spoken on the bug was Sicilian, and at the time, the Bureau agents who were listening did not have a foreign language capability, so they simply listed them as "unproductive", because they didn't know what was being said in Sicilian.

Frankly, Mr. Clark, when I hear your public statement and read the Parker study, I wonder if you would explain to us how you reached your judgment. The study doesn't seem to support it.

MR. CLARK: Obviously—how many prosecutions do you find? Zero; isn't that right?

MR. BLAKEY: Yes, but that is because—

MR. CLARK: Was Valachi productive? Could you get clippings from the *New York Times* and get more? Are you talking about a murder that has been reported and police have been working on for years? Do you call it productive because someone recited it on the telephone?

By "productive," I mean a device that leads to a prosecution. They got zero from it.

MR. BLAKEY: Let me understand your position. You are not saying it's unproductive in the sense that it does not obtain evidence of intelligence value and evidence of crime. You are saying, that since it was unlawful, it was unproductive?

MR. CLARK: No, I am not saying that. You see, you assume the FBI was gathering it for its health at the time. I assume they were gathering it for the purpose of prosecution. And there is every indication that that was so. And there were never prosecutions emanating from it.

MR. BLAKEY: It is my understanding that it was put in and kept in for intelligence purposes, to identify the major figures in organized crime, their structure and interrelationship in our society.

MR. CLARK: It is incredible they had this great academic interest in the years they weren't filing any cases and did nothing about it. I don't know how—I just don't know what reason there is to believe there was some discipline that would say, "We'll gather this for intelligence, but even learning of murder where we couldn't prosecute or where we now have evidence, we would forego it." That is contrary to experience.

MR. BLAKEY: Let me go back to what I thought the central issue before us was, whether society could expect, if it authorized a court-ordered system, at least consistent with the present Supreme Court cases, that the use of that electronic surveillance would produce evidence at trial.

Now, I have understood your previous statements about "it is unproductive" to mean that if society had authorized that court-ordered system it would not be productive of convictions—and useful convictions, high-level convictions.

Do I now understand your testimony when you said electronic surveillance is unproductive to be that you confined it to the period prior to 1968 when it was being done unlawfully?

MR. CLARK: Certainly not. I have said just the opposite.

There is no question that you and I could walk over to New York Avenue, pick up some equipment, go up to New York City, and in 48 hours pick up hundreds of phone calls that have to do with bookies, couldn't we? But you don't need that. It is a very expensive, it is a very wasteful, it is a very inefficient method of gaining information that you have crawling all over the place.

Why would you do it? It is wasteful; it is non-productive; it is inefficient at every level that I have ever seen it.

MR. BLAKEY: How do you mean it's unproductive?

MR. CLARK: Have you seen the cost of these things?

MR. BLAKEY: Yes, I have. But how much is un-productive? Are you saying it does not get evidence?

MR. CLARK: It might be productive in the sense that it reproduces something that you already have. You knew it was a bookie joint before you put the tap on, before you put the bug on.

MR. BLAKEY: Did you know all the participants?

MR. CLARK: You can pick it up from customers calling in.

MR. BLAKEY: Frankly, Mr. Clark, it's not a function of our discussion to bring out what my views are, since in this context they are largely irrelevant. I am trying to clarify our record so that those who come behind us can read to see what your judgment has been and the basis of it.

Do I understand what you mean by "nonproductive" that it is not productive of new evidence? It is your judgment based on what you know about electronic surveillance that it's not productive of new evidence, that it is merely reproductive, tells you something you already knew before you put it in?

MR. CLARK: That is certainly a major part of it, yes. You are supposed to know something before you put it in anyway.

MR. BLAKEY: You should have probable cause or you shouldn't put it in. But simply for the record I would indicate that some of the case studies that have been given to us have indicated that it's been extremely productive in identifying new people, getting evidence against people that they did not have usable evidence against when they put it in.

Is that contrary to your experience?

MR. CLARK: Yes. I mean, look at the place where it's been used without inhibition for years, and ask yourself whether organized crime is flourishing there. It is just not the method that has to be used to do the job. It is inefficient, wasteful, corrupting, and harmful.

MR. BLAKEY: What I am asking about is now limited to productivity, is it not useful?

It seems to me of all the things that can be said about wiretapping and electronic surveillance—that it is unproductive and not useful—is something that cannot be said. All the people involved with the process on a day-to-day basis say it's an extraordinarily able tool for gathering evidence. It may be grossly immoral, but at a minimum it is productive.

I have no further questions.

MR. CLARK: I really disagree with the idea that everybody says it's productive. The outcome from wiretapping and bugging in proportion to the input

in resources and time is minuscule compared with other methods. It is not productive and it is not efficient.

MR. BLAKEY: Again, the testimony of experienced FBI agents who have been before this Commission is that sometimes it is very expensive and very costly, but the same amount of time and effort spent in usual investigative methods would not have been successful; that as expensive as it is, it is the only way to get the job done against organized crime.

MR. CLARK: Well, that is a conclusion I cannot accept.

MR. BLAKEY: The evidentiary basis on which you say you cannot accept it is, I take it, the Carey Parker study.

MR. CLARK: Why do you say that? I have said we reviewed hundreds. I cited the Carey Parker study as an indepth study of 12 of them. I have never been an FBI agent or a detective or a prosecutor.

MR. BLAKEY: Thank you.

CHAIRMAN ERICKSON: Professor Remington.

MR. REMINGTON: Mr. Clark, you testified that in your view this Commission should be concerned with the maintenance of freedom, and all of us agree with that, and I take it that one of the freedoms is not to be listened to. But there are other freedoms, such as the freedom not to be subjected to a physical search or stopped and frisked on the street.

MR. CLARK: Or bugged.

MR. REMINGTON: With regard to some of those, the freedom not to be subjected to a physical search or the freedom not to be arrested unless there are adequate grounds for making the arrest, we do have provision for doing that lawfully. In other words, we have a provision which not only allows the court to issue an arrest warrant, but, indeed, in the Federal system we presently allow arrest without a warrant, even in circumstances where a warrant may have been obtained. And without regard to search for physical evidence, protected by the Fourth Amendment, we allow the court to issue an authorization to a law enforcement officer under appropriate circumstances to conduct that physical search.

I take it that you see something different in those two situations, arrest under Rule 4, for example, and a physical search under Rule 41 on the one hand, and electronic surveillance on the other.

I assume it is your view that it is appropriate under some circumstances, with judicial authorization, to make arrest and it is appropriate under some circumstances to conduct physical search. But I take it, it is your view that it is inappropriate,

even with judicial authorization, to conduct an electronic surveillance.

What I'd like to understand more clearly than I do at the moment is what the difference is. All of those involve important freedoms.

Is one less attractive as testified to, or is it that privacy involving the freedom of not being overheard is more attractive, as some have suggested? Or is it that one is more likely to be abused than the other, as some of your testimony seemed to suggest? Or is it that one, if he were skeptical, would assert one involves people of upper class and wealth and the other involves, by and large, poor people?

MR. CLARK: Well, it is a mixture, as your question suggests. But primarily it is the secret nature of it, the power and reach of the invasion. I mean it was in the infancy of its technology in a way when Brandeis described how pitifully inadequate even the general search warrant was compared to wiretap, and look at the capacity now. It leaves no place to think or be yourself or say what you will.

And in our urban technologically advanced society, we have to recognize the new needs of the individual in terms of privacy, new capacities to invade. The old search is a physical phenomenon which we can see and know about through history and has limits.

The other can watch you all the time and hear you all the time, and its capacity is enormous when you think of the capacity of electronics and computer storage and all.

I think we have to face that and say this society can and will live without it because there is perhaps no other way to maintain the integrity of the personality of the individual.

MR. REMINGTON: Your advice, then, is that this Commission really ought to focus in large part not on the question so much of whether the electronic surveillance warrant is more effective than a search warrant, which might be more effective than an arrest warrant, but rather on the question of which poses the greatest threat to freedom. And I take it it is your view that the electronic surveillance warrant poses a much greater threat to freedom than does either the arrest warrant or the search warrant.

MR. CLARK: I feel that very strongly.

MR. REMINGTON: I ask that because if you put yourself to the task of proving that search warrants reduce crime, it would be very difficult to do.

MR. CLARK: Of proving what?

MR. REMINGTON: That Rule 41 has reduced crime in that fashion.

MR. CLARK: Since crime hasn't been reduced, yes.

MR. REMINGTON: And I take it in your view a distinction between Rule 41 and Title III would not be because either has reduced the crime, but rather whether Rule 41 or Title III poses the greater threat to freedom.

MR. CLARK: I think you should consider, too, the relative efficiency—productivity, if you want to use that word. I would find it first adequate, but I also believe that the others are measurable if you can determine them.

My experience tells me that the wiretap and the bug are the least efficient.

MR. REMINGTON: If one were called upon to prove that protections against people being arrested are more effective than protections against people being listened to, I would myself find it difficult to come up with evidence that we have devised a system for keeping people from being arrested that is more effective than the system we have devised for preventing people from being listened to, if that is indeed the task of this Commission.

MR. CLARK: You always know when you are arrested or you learn about it when you regain consciousness. You don't always know when you are bugged. And there are people throughout this city and throughout this country whose lives are altered by their assumptions that they are being bugged.

I remember a recent President who said, "If there hasn't been anything wrong, they shouldn't have to worry." You remember a more recent chapter in that history, too.

You don't have to put up with that. It is a free society. There have to be arrests as long as you have anything that resembles our system of criminal justice. There have to be arrests. Those who work in that vineyard have to strive to be as sure as you can be sure in life that there is probably cause for that arrest, that there is fair and expeditious treatment of the allegation.

But with wiretapping you never know. You never know for sure, because of its nature. It is secret, pervasive, and far beyond the search warrant. And I find many abuses constantly in professional investigative agencies of search and seizure provisions. Because you know you figure out pretty soon if you have been searched and your property seized. I don't find it affecting us in the way that the other can and does.

MR. REMINGTON: This will be my last question. The significance about not finding out about it is what? As you say, I find out if I am arrested but I suffer endlessly by having that arrest record. Given the choice right now between being arrested and finding out about it and being listened to and not finding out about it, I think I'd choose to be listened to and not find out about it.

MR. CLARK: Well, I wonder—with this aside: As far as I can tell, the rule of law depends upon its possessing qualities that are inherently respect and trust of people. And wiretapping and bugging are inherently disrespectful, in my judgment, but beyond that, undermine trust, because you can't see them. You don't know about them. And I think we pay a heavy price from that erosion in this country today.

MR. REMINGTON: Thank you.

CHAIRMAN ERICKSON: Judge Shientag.

MS. SHIENTAG: Thank you, Mr. Chairman.

General Clark, your whole career has been characterized by concern for the rights of the individual, especially the little individual who wouldn't ordinarily be protected. And you have a great deal of respect for the dignity of the human being.

Now, in connection with that you have testified that to use the bug or wiretap is an inefficient way of getting information that would tend to incriminate someone.

Is it really because it is an unfair means, contrary to the dignity of man, or is it because it is inefficient that you are opposed to it?

MR. CLARK: Well, in my judgment it is both. The more important value to me, because we are getting very good at being inefficient, is the moral issue.

MS. SHIENTAG: The moral issue is the big one?

MR. CLARK: Yes.

MS. SHIENTAG: Because we have had testimony before us, some from the attorney who handled the *Giordano* case where 600 wiretaps were found to be improperly authorized, and he said it was such an inefficient way that he was opposed to wiretapping, and he had had extensive experience in criminal law. I am talking about James Hogan.

MR. CLARK: Who was it?

MS. SHIENTAG: His name was Hogan from Florida, the attorney who had the original two cases that went to the decision of the Supreme Court in *Giordano*.

MR. CLARK: One comment that I can make on that—you see, I remember the political struggle in the Department of Justice. I always tried not just to tolerate, but to stimulate the expression of ideas. The prosecutor may have been Mr. Blakey who wrote that about its being the most productive source.

MR. BLAKEY: For the record, it wasn't.

MR. CLARK: It would have been nice if it had been; I'm sorry, it would have been interesting.

As a prosecutor, what is experience? What does the prosecutor see? Sometimes his vision becomes

the evidence in his case and that's it. That is almost the outer limits of what he sees.

What does he know about all the things that the investigators did in the case. What does he know about all the efforts of wiretapping, the installations?

What he finally sees is the end product. What does he know about all the other investigations where they were used and nothing happened. What prosecutor really knows? What prosecutor in the United States really knows what his local police departments are doing?

MS. SHIENTAG: Well, the assistant D.A.'s often direct the agent on what evidence they need and how to acquire it. And you should know that very well from your position as Attorney General.

MR. CLARK: I had a little bit of perception. I think the FBI, for very many reasons, has little confidence in the U. S. Attorney's office. I have great confidence in the office. I think it's great. And Mr. Hoover would constantly say, "I am not going to turn this material over to the U. S. Attorney." When they went through all the years of bugging in the late '50's and early '60's, they did not confide in the U. S. Attorney. The U. S. Attorney couldn't name the chiefs of half the bureaus in his district, probably. And the U. S. Attorney who said he knew what the FBI and other agencies were doing in the way of wiretapping is actually relying on faith, which is what you have to do in a situation like that.

MS. SHIENTAG: There are various kinds of crime like there are various kinds of people. There is the street crime, the husband beating the wife, the corporate executive suite crime; there is big syndicate crime, big business—big situations, in the same way there is bigness in corporations and activities of big law firms, even. And the very bigness is what makes the people in some cases—the cartels and organizations.

Don't you think the same thing should apply in respect of big syndicates of crime, that every measure should be taken to stamp it out, just like we would an antitrust action?

MR. CLARK: Well, as long as I have had a romance with antitrust, I'd give a higher priority to stamping out organized crime. The knowledge of technology escalates. We learned about it after the fact that some of the organized crime operations got very skillful at their own technology, jamming devices, and so on. So where do you go?

MS. SHIENTAG: You have to fight fire with fire?

MR. CLARK: No, you don't fight Fascism with Fascism. You live by decent standards and pay the price.

MS. SHIENTAG: You pay the price?

MR. CLARK: There is a sizable price attached.

CHAIRMAN ERICKSON: Chief Andersen.

MR. ANDERSEN: I have no particular questions, but your statement that prosecutors do not know what the police are doing is 100 per cent accurate, as far as I am concerned. Prosecutors do not know to a considerable degree.

I have just listened to your position very carefully, and it is the broadest position that has been put forth to this Commission in this general area.

And I have no questions. I just wish to say thank you for appearing.

CHAIRMAN ERICKSON: May I ask a few other questions, General?

MR. CLARK: Surely.

CHAIRMAN ERICKSON: As I understand it, one of the reasons you are so opposed to wiretapping and bugging is that it is done in such a way as to destroy a person's expectation of privacy. Would that be it?

MR. CLARK: That is the phrase that is used.

CHAIRMAN ERICKSON: That came from *Katz*—and that the purpose was to protect persons and not places.

Professor Remington went into Rule 41 and there the magistrate in determining whether the invasion of privacy which will be made has the benefit of examining the affidavit and materials that have been compiled before he enters the order directing that this right of privacy be invaded.

And as they said in *Berger*, it is difficult to predict what a conversation is that hasn't occurred yet.

Is that one of your objections?

MR. CLARK: Yes. And under Rule 41, you are supposed to state with some specificity, and you go in there one time and that's it. It is a wiretap, and how many conversations, how long, are you waiting for?

CHAIRMAN ERICKSON: Let's take the next step. As far as telephone conversations are concerned, is there really any expectation of privacy when you telephone anyone? We all know that there are extension phones and certainly when you call in to the average law office, that could be picked up by any lawyer in any one of the offices.

So when you speak over the phone, do you have a right to expect privacy, in your opinion?

MR. CLARK: When you are talking about the right and expectation of privacy, I think there is something conceptually limiting about the notion.

We live in a world where you need constantly to communicate with people that are at some distance. In the past you could walk out in the pasture and stand under a tree and walk around and make sure there was nobody behind you or up in the tree, and live in confidence there.

We live in a technologically advanced mobile society. We need to be able to talk to people in confidence.

So my wife is in New York; I want to talk to her. I'd like to think I could do so without somebody hearing what I have to say, because we have things that are personal to us.

And I think society needs to create that right and that sense that it is protected by privacy in communication from electronic surveillance.

CHAIRMAN ERICKSON: When Title III was drafted, they wrote the *Rathbun* exception into the statute which would permit someone to overhear a conversation by using an extension telephone, if it was done with the consent of one of the parties. And that has been a pretty well-recognized exception, and ever since that decision was announced many years ago, it was the theory that one party, when he consented, was not really depriving anybody of any rights when he consented to his own conversation being overheard.

That goes to the question of: Just how much can any of us expect by way of privacy in our communications in today's society?

MR. CLARK: Well, you can't expect any, but you ought to be able to, and it would be a healthier, stronger society if you could.

The reason you can't expect it is our fear of surreptitious overhearing.

But I have gone through a process of change. The *Schwartz* case came out of my home town of Dallas where I was practicing law. And Morrie Hughes came up to argue it and I felt very strong about it. He was strange in what he was trying to say, that *Schwartz* had an expectation of privacy, even though that language wasn't used at that time—even as someone was recording as he was talking to them.

But as I have watched the nature of our society you see what it means in assemblies and meetings for one person to go in—there are dozens of people saying different things, holding little conversations here, there, and elsewhere, and one person, when it comes to defense conferences—if there is any place we have to have some hope for integrity, if you are to have justice, it is in defense counsel.

You take a Gainesville case; you take a Camden case; you take a Harrisburg case; you take an Attica case where you have scores of people involved—and you can't know who they are. This guy has a right to his lawyer; this guy has a right to his lawyer. You people have volunteered on the case. You don't have any money.

And one of them is rigged and you have violated the others.

CHAIRMAN ERICKSON: What I was getting at was in a jail if a person is talking to a cell mate that is perhaps a disguised police officer, he has no right to expect privacy in the confines of the jail. There are a number of cases that have dealt with that.

MR. CLARK: I see. You are writing the law. You need a *Massiah*—

CHAIRMAN ERICKSON: Of course, this Commission cannot act as a court in passing upon anything, but we are just trying to make recommendations as to what the parameters ought to be and how effective this has been, whether it has protected privacy, whether it has carried out the aims that were set forth.

MR. CLARK: Your duty is not merely to interpret the law. Others can do that. But your duty is to define actual policy of the United States within the law on this subject.

And I feel awfully strongly about these things, but just watching what it does in prisons—the fear of overhearing is an incredible thing. I wonder how many inmates have been beaten up or worse because someone decided they were doing something. And that is just not the type of society we want to create.

CHAIRMAN ERICKSON: You think this right to privacy should even be expanded to the prisons?

MR. CLARK: Oh, sure.

CHAIRMAN ERICKSON: So you couldn't hear what the prisoners are saying in their cells?

MR. CLARK: Who needs them? You shouldn't have them there unless you think you can make your case. You are not going to try to make your case by his mouth after you capture him. That would seem to me to be a political, inadequate way to approach this thing.

But this is something we have worried about for years. Why didn't the FBI put a bug on Lloyd Douglas in the Berrigan case? Or did they? I have had people from the Department of Justice say, "This is hearsay." Here is a guy that is an informant on June 4, 1975, and everything that led to the alleged plan to kidnap Kissinger. They bugged Lloyd Douglas later and their technology was so poor that when it was played in court they couldn't even hear half of the conversation.

Maybe they did bug him. A lot of people think they did.

What about the phone conversations in and out?

CHAIRMAN ERICKSON: That has been pretty well condemned from *Coplon* and *Mapp*.

MR. CLARK: I would hope so, but who has much confidence in it? How many lawyers talking to an inmate from prison will really speak openly?

CHAIRMAN ERICKSON: I don't think any of them would.

MR. CLARK: So—

CHAIRMAN ERICKSON: So there is no expectation. As a defense lawyer, I wouldn't talk.

MR. CLARK: We want to live by government rules and you won't talk.

CHAIRMAN ERICKSON: You made that point and made mention of the fact that people in communications don't communicate freely among themselves because of the fact they think they are being overheard. So how can you say there is any expectation of privacy?

MR. CLARK: One day—you don't want to use this—I was driving home with a Justice of the Supreme Court, no relative of mine. And he stopped the car—he was driving—and said, "I want to tell you something. Let's go over here."

I said, "Okay."

And we got out of the car. And he said, "I'm afraid my car is bugged."

We have seen polls among members of Congress. I had 30-odd congressmen call me up—George Brown was a congressman from California at the time. We had 30-odd congressmen, and they thought they were being tapped. You can say, "Darned right, they think they are being tapped, and they are."

CHAIRMAN ERICKSON: Do you feel there is a sense of paranoia in any of this?

MR. CLARK: Oh, sure, absolutely. People ask me if I have ever been tapped. And I don't think I have ever been tapped.

I know I have been overheard. I was trying to get to the Leningrad trials, so I called Ambassador Dobrynin several times, and within a year Jack Anderson has a column on it. This is the price you pay for this sort of thing. His column begins that he had material leaked to him from the White House, and it shows that Ramsey Clark had been tapped. And then he has a few quotes from the phone conversation. The only thing he had mixed up was it wasn't me that was tapped; it was the Russian Embassy. He just had it backwards.

There is a lot of paranoia about it.

At least, I think he had it backwards.

[Laughter.]

CHAIRMAN ERICKSON: We talked about surveillance techniques. Many jails, I think, are conceivably bugged, so they can hear what is going on in the cells, and very often they hear confessions or admissions being made that might be in violation of the *Massiah* case that you referred to.

But doesn't it also come about as part of the security problem in providing safety within the jail?

MR. CLARK: I think there are people that sincerely believe that. I don't. I think it makes for a more dangerous situation. I think you increase frustrations and anxieties. I can think of at least three

cases now where I have sought court orders—I have never gotten one—to permit conferences outside the prison between counsel and the accused, because you can't prepare your case. You are not willing to talk, whether it is Danbury or San Quentin.

I just don't think that is conducive to peace in prisons or justice outside. I think it creates a great deal of frustration and trouble, and I think as a security technique it has no value.

I think it is not worth it. There are other means of being secure.

CHAIRMAN ERICKSON: General Clark, we are extremely grateful to you for being here.

I might say that we honored your time commitment and unless there are other questions from any members of the Commission, we will say that your testimony will add immeasurably to the study of this Commission and be given full consideration in drafting the final report, and we hope that we can come up with recommendations that will not only work toward effective law enforcement but toward protecting our privacy.

MR. BLAKEY: Mr. Chairman, I wonder if I could add a note of appreciation to General Clark for being very patient while a law professor asked long, complicated questions. I appreciate your candor.

MR. CLARK: I thank you, too, Mr. Blakey, and Mr. Chairman, and members of the Commission.

CHAIRMAN ERICKSON: Thank you again for coming.

At this time we call Professor Greenawalt.

[Whereupon, Mr. Greenawalt was sworn by Chairman Erickson.]

TESTIMONY OF R. KENT GREENAWALT, COLUMBIA UNIVERSITY

CHAIRMAN ERICKSON: Before proceeding, the record should reflect we are honored to have with us Professor R. Kent Greenawalt of Columbia University. He has authored a law review article on consensual surveillance that appears in the 1968 *Columbia Law Review*. He is an expert on the topic and is currently consultant on electronic surveillance matters for the White House Office of Telecommunications Policy and the Committee on Privacy.

Do you have some preliminary remarks or an opening statement?

MR. GREENAWALT: I'd like to make a very brief opening statement.

I thought I would say a couple of things about my background and then summarize very briefly what I have said in the report which you have copies of.

The report was done for the Office of Telecommunications Policy and the Domestic Council Committee on Privacy.

What I was asked to do was a general study of legal protections of privacy. The sections you have are the material that is directly relevant to your inquiry, but that is only a small part of the report. The entire report will be reproduced and circulated in around a week or two.

CHAIRMAN ERICKSON: Will a copy be made available to us?

MR. GREENAWALT: Would you like one?

CHAIRMAN ERICKSON: We'd appreciate one.

MR. GREENAWALT: I will ask them to send a copy to you.

I think the only other relevant experience besides what you mentioned is that I was a member of the Subcommittee of the Committees of the New York City Bar Association which did a report on the 1968 Act as it was going through the legislative process. And in 1971 through 1972 I was one of three Deputy Solicitors General; and in that capacity I did review all the criminal cases that were coming up to the Solicitor General's office.

My general perspective about electronic surveillance is that it is a serious threat to privacy and should at least be sharply limited. I am not at all sure there should be any authorized wiretapping and electronic eavesdropping, putting aside national security matters; but the criticisms I make in this report are directed more at specific parts of the statute.

On page 25 I summarize my view, "Even if one accepts the need for some eavesdropping, the act is still subject to attack for permitting too many persons to obtain orders in too many courts for too many offices and for too long a time."

I will now simply enumerate the specific criticisms or recommendations I make, and then we can discuss those which interest you most.

First of all, I think the number of crimes which can be the subject of surveillance should be sharply cut back. I do not believe surveillance should be routinely allowed for 30 days. I think a much shorter period should be the maximum, with the possible exception of situations where a phone is not used for private conversations. If there are situations where a phone is thought to be used only for gambling transactions or something else, then the notion of this longer surveillance doesn't bother me. But if the phone is a home phone or an office phone, then I think 30 days is really too long.

It goes without saying that I also think the renewal period provisions are much too relaxed under the present statute.

The other exception I might make to what I have said about the long period of surveillance is if there is some matter of extreme urgency, let's say a kidnapping in which a life is in danger, or something like that.

Whatever is done about wiretapping, I think that placing bugging devices in homes or offices is even more intrusive of privacy, and I think it should be more sharply restricted. The present statute doesn't draw a distinction between the two, but I think bugging is an even more serious threat to privacy.

I think even fewer officials should be permitted to approve applications. The rules about the Federal Government are adequate in terms of who can approve the applications, but the rules are too relaxed in regard to state officials.

I think fewer judges should be allowed to issue orders. Judge shopping is possible now, and it should be possible to designate only a few Federal judges and require that all eavesdropping orders go through those judges.

I think that there should be no authorization for emergency surveillance—perhaps I am wrong about this, but it seems to me unlikely that there will ever be circumstances in which it will not be possible to get a rather quick authorization from a judge; that is preferable to having emergency surveillance authorization which apparently is not being much used anyway.

In regard to the notification that is given after surveillance takes place, I think that persons who have been the object of surveillance should, as a matter of course, be able to see the order, the application, the records of conversations that are taken, whether or not they are being prosecuted. That would give them more access than they presently enjoy under the act.

I have somewhat more doubts about the suggestion I am going to make now, but I also think that when the other parties to conversations are known—that is, not the people who are the objects of surveillance but the other parties to conversations, those parties should also receive inventories as a matter of course.

I think the present act provides for postponement of the inventory in a rather open-ended fashion, and there should be some clearer termination point for postponement of the inventory.

The act should be extended to digital transmissions. As Arthur Miller has stated in his book, the present language doesn't cover that.

I think either the present statute should be extended to pen registers, by which you find out what number a person is calling rather than getting a conversation, or some other legislation should cover pen registers.

Possibly some other legislation would be appropriate, because, while this is a matter of some concern, pen registers are not as intrusive on privacy as interceptions of actual conversation. You might have some broader sort of allowance in terms of this law enforcement device than for ordinary interceptions.

My own sense is that police listening at extension telephones and at private switchboards, which I think are not covered by the present act, should also be subject to regulation.

Those are my recommendations as they relate to surveillance where neither party to a conversation recognizes that the surveillance is going on.

What I have to say about situations in which one party to the conversation either takes in a recording device or some kind of transmitting device is really boiled down in a couple of recommendations.

I think law enforcement monitoring of the kind when an informant takes a bug in with him to a conversation should be allowed only on a court order. The split in the Supreme Court in *United States v. White*, holding that warrants are not required, was five to four. I believe that the position of the dissenters should be adopted as a matter of statutory law.

Since this use of electronic devices does not intrude on privacy as much as third-party surveillance, I think it would be possible to allow it in a much broader range of cases than third-party wiretapping.

In terms of a private person recording a conversation without the knowledge of other parties to the conversation, the present approach of the statute is to permit that unless the monitoring is being used to commit a crime or tort or some other injurious act. A preferable approach would be to say that private monitoring of this kind should be forbidden unless it falls into one of a number of specified categories in which it would seem to be more socially acceptable.

This is something that I discuss at some length in the report that you have. Very briefly, I think the kind of situations in which a person should be allowed to engage in private reporting of a conversation unknown to the other party would be when he is trying to establish that the other party is engaged in some wrongdoing, when he is trying to protect himself in some way against an inaccurate account of the conversation, when he is trying to engage in some form of treatment—I mention in the report the possibility that a psychiatrist might record a patient's conversation in order to have an accurate recollection of the conversation, but not want the patient to know he is doing so, because it might destroy spontaneity—when he is trying to make

scientific observations, and finally when he is engaging in service or supervisory observations.

Telephone companies, to take one example, monitor some conversations between operators and callers so they can make sure the machinery is working properly, and also so they can make sure their operators are giving the right kind of advice. The same kind of thing is done by the Internal Revenue Service.

So I think the preferable approach to this kind of private monitoring would be to try to designate the kind of situations in which that kind of monitoring does seem socially acceptable or at least is a borderline question, and to say it is permissible in those situations and forbid it in all other situations.

That is all that I have in the way of introductory remarks, Mr. Chairman.

CHAIRMAN ERICKSON: Thank you very much.

Professor Remington.

MR. REMINGTON: One of your suggestions was that the number of crimes be more limited than they are currently in Title III; is that correct?

MR. GREENAWALT: Yes.

MR. REMINGTON: One of the problems I think we become aware of in attempting to react to a suggestion of that kind is the fact that very often the definition used for the purpose of enacting a substantive criminal law may or may not coincide with what law enforcement may believe to be the objectives of the investigation. In other words, the target may not be something defined by the substantive criminal law as a particular crime.

Therefore, the question I ask is whether, as you see it, there is any alternative to listing specific statutory crimes in order to achieve the objective which you recommend, which is to limit electronic surveillance warrants to situations where they are actually needed.

Is there an alternative to just listing—kidnapping, murder, gambling—citing the statutory references?

MR. GREENAWALT: Let me take that in two stages, if I may.

First of all, given my general perspective about electronic surveillance, I am not sure that I would accept the presupposition that if there is no specific serious crime and you think somebody is organizing general criminal activities or engaging in serious incidents of some crime that is considered a minor crime, it should be all right to engage in electronic surveillance.

For myself, I would be willing to accept the notion that some of those people would not be subject to electronic surveillance if the crimes for which surveillance was possible were sharply limited. But assuming I am wrong about that, and the presup-

position in your comment is right, that there are occasions when you want to allow electronic surveillance in that kind of situation, it seems to me it is very hard to write that flexible approach into a statute. This is the kind of thing that can be done administratively, a prosecutor or Attorney General or the Director of the FBI can say, "There has to be a link between this person and something that is really a serious law enforcement concern, and we are not going to have eavesdropping unless that kind of connection is made." But it is awfully difficult to think of what kind of language you could write into a statute to accomplish that.

MR. REMINGTON: The reason I ask the question is I think we have typically been fairly unsuccessful when we have tried to limit authority by enumeration of crimes, whether that is in the area of felony murder, for example. There have been efforts on the part of some states to indicate what would happen as a result. I think that has been true in some states in terms of self-defense where they provide you can use self-defense only with regard to certain enumerated crimes.

I think much of this is searching for a principle that ought to control in the case of felony murder, if there be such an offense, or in self-defense or in things of that kind.

I am wondering whether our current situation in the area of electronic surveillance, to the extent there is to be legislation at all, will be in the area of scholarship, that anybody who has been able to identify with sufficient care the permissible objectives of electronic surveillance, assuming there are to be some permissible objectives—whether it isn't just, as I say, the result of that default that we have to open up the statute book and go down a long list. And once you do that, isn't it inevitable that the list will have to be longer than anyone wants, in order to cover the area which you have not been able otherwise to identify?

Isn't that the experience which we have had in almost every case—the inability of the law enforcement to use force in effecting an arrest? And there are others.

MR. GREENAWALT: I would be inclined to think that it is not a failure of scholarship but is the inherent difficulty of the problem. It seems to be that about gambling there is fairly general agreement that if wiretapping is justified in terms of gambling offenses, it is because gambling is tied to organized crime, and organized crime is a very serious threat, and so on.

Now, people have some vague idea what organized crime is and what organized crime is not. If I were sitting down with somebody as a chief prosecutor I could ask him: Does this have to do

with organized crime? What is the connection? And so on and so forth.

Let's assume the wiretap is okay for that, which I have doubts about. But I am not sure that makes it easier to write into the statute or even that it is an appropriate kind of distinction to make in the statute.

So the problem you are talking about is a real one, but I think it may be more in the nature of the problem rather than any deficiencies which any of us are able to correct.

MR. REMINGTON: Well, if I understand you, what you are really saying to me will result in overly broad legislation with the hope that there will be administrative self-restraint. Because it seems to me inevitable if you say that one cannot identify the permissible objectives of electronic surveillance legislatively because we do not have the capacity to do so, given the complexity of the subject matter, then having conceded that, one is driven to the point of enumeration which would leave room for the use where it ought not to be, with the hope there would be administrative self-restraint.

MR. GREENAWALT: That is where I would be led if I accepted the presupposition that some of these things which aren't in themselves subjects of serious crimes should be the subject of surveillance. If you asked what I suggest on the basis of my present knowledge, I'd say okay, maybe there are some of those situations where wiretapping and eavesdropping would be justified, but since it is so hard to spell them out we will not allow it at all for those crimes. And I'd prefer a very narrow category of crimes—murder, kidnapping, bribery—maybe one or two others, but something very narrow, and acknowledge there would be a lot of other situations in which wiretapping would be useful, but we just wouldn't use it.

MR. REMINGTON: If one goes in the direction of murder-kidnapping, and with a permissible use of electronic surveillance, I take it, given the kind of testimony we have had, that most of the people feel that these are crimes for which wiretapping is not technically effective, because they are by and large "history" crimes, and though this may be an exception in the case of kidnapping, the need is not for dealing with traditional crimes, but rather dealing with ongoing conspiracies.

Were one to limit it to murder, kidnapping and bribery, one would exclude the whole narcotics area.

I am not certain whether you are saying that it ought to be impermissible to use it in narcotics, or whether you are saying that is a price of my inability to adequately define the target, and I will be less than an authority because I can't define it.

MR. GREENAWALT: About narcotics, I would think the latter. I think there are probably some conspiracies that are involved with narcotics that are so substantial and so serious that if you pointed to that particular conspiracy against these particular people and asked would I think the use of eavesdropping morally justified, I'd probably answer that "yes." I am not sure I'd feel that way about gambling, but I would about some narcotics enterprises. But I would say there are so many other situations in which eavesdropping probably isn't justified, that because of my inability to define it I'd prefer to see it not covered by the statute.

CHAIRMAN ERICKSON: We will take a five-minute recess.

[Whereupon, a short recess was taken.]

CHAIRMAN ERICKSON: Professor Blakey.

MR. BLAKEY: Professor Greenawalt, I wonder if I could explore not all 15 points you made but one or two of them.

You offered a general suggestion that the renewal process was too relaxed. I wonder if I could explore what you mean by "too relaxed."

Would you suggest that there be a fixed number of renewals, two, three, four, or five, or an outside limit of the number of days?

MR. GREENAWALT: Of course, I suggested that I thought the 30 days was probably too long to begin with.

MR. BLAKEY: Well, it seems to me that issue is really subsumed in the renewals. If you have unlimited renewals, it really doesn't make any difference what the initial is. I'd really rather discuss it at the renewal point rather than the initial surveillance point.

MR. GREENAWALT: I was thinking of a much shorter period of time. I was thinking with no renewals. Barring the exception of some extraordinarily important matter involving a danger to life or something like that, or a situation in which you were only wiretapping a telephone in which there were no private conversations, probably wiretapping should not be permitted unless you have really very specific information that a conversation is going to take place within a day or two days, or something like that.

I am not really being responsive, but that would sort of take care of the renewal problem if you bought that.

If you don't buy that—

MR. BLAKEY: Frankly I never really understood your objection to the continuing character of surveillance. It seems to me the initial issue is should you put it in at all, but once you have put it in, and it no longer ceases to be a question of probable cause, you have actual persons on that phone or in

that room and you have actually heard a number of people who are innocent or a number of people who are guilty. The judge, on the issue of renewal, is really not speculating any more, at least not in the abstract way he was when it was initially put in. You know more or less who you are going to hear; you know the character of the phone. It seems to me as long as concretely you don't have a disproportionate number of innocent conversations being unnecessarily overheard, it should be all right. The longer you listen and identify the people who are not incriminating themselves—the baby sitter, the wife, the mother-in-law who lives there—the easier it is simply to shut off. So the truth is the longer you listen, the more sophisticated you can be in limiting it to a very narrow intrusion.

Am I wrong in that analysis?

MR. GREENAWALT: I think as far as it goes, that is probably right. There are, of course, conversations which involve some private matters and some matters that aren't private, so even by knowing who the person is, if that technique is working perfectly and you are only listening to people who are involved in crimes, if the person has a perfectly private conversation you listen to that.

MR. BLAKEY: No, the theory of the statute is if you hear a person speaking about something you are not supposed to listen to—

MR. GREENAWALT: After you have listened to enough to be sure he is not going to start talking about another subject.

MR. BLAKEY: And after that, you are permitted to sample in.

MR. GREENAWALT: I have not kept up with this technology.

MR. BLAKEY: The other issue I raise with you is the 30-day surveillance. You are on the 30th day and you only allow 30 days of surveillance, and they say, "Call me tomorrow and I'll give you the name of the hit man and place where the hit will happen."

MR. GREENAWALT: Then you should obviously have a renewal.

MR. BLAKEY: Or, "Call me tomorrow and we will identify the big boss."

MR. GREENAWALT: Yes.

MR. BLAKEY: And once you begin recognizing that in the latter part of surveillance you have continuing objectives to pursue which are within the range of reason, this notion that there ought to be stricter rules on renewal seems to disappear in your exceptions.

MR. GREENAWALT: Yes. Of course, now renewals can be asked for on the same basis as the original authorization.

MR. BLAKEY: If you have no better probable cause than you had the first time, that would be an abuse of renewal, it seems to me.

MR. GREENAWALT: Yes.

MR. BLAKEY: If you can show no productivity—you thought you had probable cause, the judge let you put it in, and you didn't hear anything—it seems to me there is a very heavy burden on the prosecutor.

MR. GREENAWALT: That is certainly not in the statute.

MR. BLAKEY: If you get a renewal, it requires the same amount of probable cause you had in the first place, and the absence of productivity in the last period of surveillance argues against surveillance?

MR. GREENAWALT: That last proposition is not in the statute itself. You obviously had a lot to do with the legislative history, you may know of something which I am not aware of.

MR. BLAKEY: One of the classic situations that arises is suppose you put it in and the first call you get is, "I am leaving on my two-week vacation. I will be back in 14 days," which is a clear explanation for the lack of productivity. I take it, then, a renewal probably would be permissible since you have explained why there was nothing coming over the phone?

MR. GREENAWALT: Yes, I think in that situation you should cut out for the next two weeks when the person is away.

MR. BLAKEY: Which is precisely what the statute requires. I take it the statute does not authorize 30 days of surveillance. It is up to 30 days of surveillance, justified as to time.

MR. GREENAWALT: That is correct. And I am not familiar with the facts about the length for which surveillance is ordinarily authorized. I guess one of the things that your commission is going to do is to find out whether the statute is being applied with all the understood limitations which you think are either in the statute itself or in the legislative history.

MR. BLAKEY: Let me move on to another issue. You expressed a preference for no emergency provisions. Is that based on an analysis of law enforcement experience or a general philosophical distaste for the absence of judicial supervision?

MR. GREENAWALT: Well, it is based in part on the latter. It is based secondarily on my understanding, which is not based on the careful analysis or lengthy reading of what actually happens. It normally takes hours to set up an electronic surveillance. If it takes that long, then there shouldn't be any reason why you couldn't get approval from a judge in most cities.

MR. BLAKEY: Would you be satisfied with a provision that said something like the following, "In emergency situations when you do not have time to fill out all the affidavits, get them typed and signed and cleared with Washington, appropriately limited surveillance may be conducted, but (not completed) before the surveillance itself is begun, so a phone call may be made to the judge's office before the surveillance begins."

Would you be satisfied with that rather than having the full process having to be gone through before you can put it in?

MR. GREENAWALT: Actually, Judge Erickson mentioned this during the break, and it was a point I hadn't thought about. The thing that would be for me very important would be to get judicial approval at some early point in time. So if you thought that an emergency provision was important, and there were only a few people in the government, in the Executive Branch, that could authorize the surveillance, it might make sense during the emergency period, however long it would be, to permit some lower officer to make the decision.

MR. BLAKEY: But the typical situation the law enforcement people have given us is that on the telephone you hear a meeting is going to take place in a hotel in an hour. And you could get to the hotel, rent an adjoining room, and bug it in time to cover the two people. But, incidentally, you wouldn't know which room they were assigned until the clerk gave them the key. So that it would be a race from the ground floor to the sixth floor to get into the next room to cover that one meeting.

MR. GREENAWALT: Well, to take the second point, which obviously is the least important, I would think the ingenuity of drafting affidavits would be sufficient so that you could designate the room next to the room in which so and so is going to check into a hotel. I would think that would be sufficiently particular to meet the requirement.

MR. BLAKEY: On a Fourth Amendment issue? I thought you had to specify where.

MR. GREENAWALT: If I were a judge, I'd sustain that under the Fourth Amendment. If you knew a guy was coming into a particular room and it was a search situation and you wanted to search his room and didn't know which particular room in the hotel it was going to be it should be all right to give that kind of description.

MR. BLAKEY: I don't agree with you, but the cases leave something to be desired on that question.

MR. GREENAWALT: Anyway, that is the lesser point. The more crucial point you are getting at is that it may be that some time you have such short notice you literally do not have a chance to get to a judge and get approval.

You see, when you authorize emergency surveillance, whatever risks there are of abuse and so on are amplified. It should not be done just because we can think of one appending case or point to one instance in history. It should be done only if the need arises with some frequency. If that is so, you might want to write a statute that says, "If you make the application within an hour or two and it is approved by a judge within three or four hours, then for the first few hours you can bug without judicial approval." I'd want it much tighter than it is now.

MR. BLAKEY: I want to raise another issue with you: Giving third-party notice, that is, to people who are not to be indicted, strangers who fell into the wiretap one way or another.

The person who is the subject of the wiretap must be given notice. The judge also has discretion to give notice to all or some lesser number of others in the interest of justice.

MR. GREENAWALT: Yes.

MR. BLAKEY: The case law indicates under that the judge should make discretionary judgment based on information given to him by the prosecutor as to the classes of other people. People to be indicted would be one class of people, utter strangers would be another, but the judge is to make a case-by-case judgment as to how many or all of these people should receive notice. Some of the cases also indicate that if a tap is thought to be unlawful, the government might have an affirmative duty to find out who everybody is and to go forward and notify them all.

I wonder if we would serve privacy well by mandating a service on all known people. Let me give you a fact situation that occurred not too far from Buffalo. They had a wiretap in on a prostitute, and the judge ordered notification to all the people who had called her. Certified letters were sent to all the families, I suppose sent to the household, to the father. And the headline in the newspaper article which reported it read something like the following, "Honey, who is Donna?"

The obvious implication of the story is that mail addressed to a man at his home sometimes becomes available to his wife.

I wonder if we would serve privacy well by giving notices to people like this "John," the patron of a prostitute or the patron of a gambling business routinely.

Wouldn't we violate more privacy, possibly rupture more family life, if we did it routinely than if we gave the judge some discretion?

MR. GREENAWALT: I think there are two issues, and I think they are both serious. As for the particular issue you posed you might say, "Okay, if it's a prostitute, if it's going to be embarrassing for

somebody to be notified in a way that somebody else in the family is going to find out, then you should perform the notice in some other way," which I presume could be done. You could take a sealed letter to the guy's office or call him up on the telephone and make sure you are not talking to his wife, and so on.

What I regard as the more serious objection was made by somebody in the Office of Telecommunications Policy when I showed them the draft of my report. That was, if you find out that your conversation with a certain person is tapped, and you are pretty sure the object of the tap was the other person, you may start to suspect the other person of something even though you have no basis for doing that. So this would sow a lot of distrust among people who work together. That is a substantial point.

Let me continue. I said I had some doubts about the suggestion when I made it. I think this is a crucial point at which, if you think wiretapping is really a generally all-right technique, you will resist the suggestion I made. I think the effect of this more general notification would be that people would have a much more accurate idea of the breadth of surveillance, and you'd have much more opposition.

MR. BLAKEY: Don't we get that from the reports that indicate the number of taps put in, the number of people overheard, and the number of calls intercepted?

MR. GREENAWALT: I think there is a big difference if you know your conversation with so and so has been overheard. I think people look at that differently. Of course, then fewer people who are not being tapped might think they are tapped than do now.

MR. BLAKEY: Let me raise a related issue with you. While our mandate is wiretapping and electronic surveillance, we have had some testimony on related techniques of surveillance and you have raised one, the pen register. I think you would support some sort of warrant process as a precondition to the use of a pen register—

MR. GREENAWALT: Yes, I can't say that is a terribly well-thought-out suggestion.

MR. BLAKEY: Would you do the same thing for mail covers? The law says you presently don't have to have it.

MR. GREENAWALT: Yes, I am bothered by mail covers, and as far as I know they are used much more extensively than I feel would be desirable. I might think that the court-ordered system is a good idea. I think there should be more regulation of mail covers.

MR. BLAKEY: Do you see a similarity between a mail cover and a pen register?

MR. GREENAWALT: I think they are essentially the same.

MR. BLAKEY: What about photographic surveillance?

MR. GREENAWALT: Photographing somebody in a public place?

MR. BLAKEY: Yes. Obviously, if it is in a private place it is a Fourth Amendment problem.

MR. GREENAWALT: No, that is not obvious, because if somebody stands across the river with a telescopic lens and photographs me in my apartment, it is not covered by the Fourth Amendment now.

MR. BLAKEY: Let's take both.

MR. GREENAWALT: If you are talking about photographic techniques which would allow people to photograph things as to which people have an ordinary expectation of privacy, I think that creates a serious problem and shouldn't be done generally.

MR. BLAKEY: I suppose what I am raising with you is do you think there is a legitimate expectation of privacy on people's part, for example, during a demonstration or at a funeral? There are instances, for example, of FBI photographing organized crime funerals.

MR. GREENAWALT: I think those present serious issues of privacy. I think the pen register and the mail cover intrude on privacy; I don't expect that the government is going to look at where my mail is going. If I am out walking on a public street, although I may hope not to be seen and expect not to be seen, my expectation of privacy is considerably less. I think it may exist, but it's less. And I would feel that way about demonstrations.

There is an example which I remember where Eldridge Cleaver was speaking at Iona College, and apparently some law enforcement body—I think it was local—took down the license numbers of people parked outside to go hear Eldridge Cleaver. I thought that was an intrusion on privacy.

While I think these things do involve substantial problems of privacy, I think there is a greater expectation of privacy about one's mail and about one's telephone, even the numbers one is calling. Exactly at which point on the spectrum we say, "Now is the time to have a court-order system," I'm not sure.

MR. BLAKEY: Do you think you ought to have a court order to get toll records?

MR. GREENAWALT: Well, I guess that is the pen register after the fact, isn't it? Yes, I would think so.

MR. BLAKEY: Do you see a problem in the difference here between surveillance by human ear, human eye, and some enhanced ability, that is, using a camera, a recorder, or a pen register, some device of that kind? Is there a real difference?

MR. GREENAWALT: Well, I would not draw such a distinction. I think it's in terms of the information you are getting. Obviously, finding out what numbers you are calling is less intrusive to one's privacy than whether a conversation is being listened to.

MR. BLAKEY: Do you think we ought to have a court-ordered system for bumper beepers?

MR. GREENAWALT: For what?

MR. BLAKEY: Tracking devices placed on the back of a car to send back electronic impulses to make it possible to follow the car, without having to do like they do in TV—being two blocks behind?

MR. GREENAWALT: I guess not, on the theory that if the police can do it cleverly, they have every right to follow your car; but I haven't thought about that.

MR. BLAKEY: As you see, I am doing what law professors always do.

MR. GREENAWALT: I am doing what law students always do.

(Laughter.)

MR. BLAKEY: I am trying to explore the parameters of how you see privacy and why you would require a court order in a number of related but not necessarily identical situations.

MR. GREENAWALT: To make the general point, I would say there are many expectations of privacy. Some are of greater importance to people and some are of lesser importance. There are some accepted rules for what the police can do now in terms of intruding on things that you would like to keep private.

MR. BLAKEY: Is this a factual question as opposed to a value question? Should we go and try to find out what people's actual expectations are, or are we trying to kind of design an ideal society where our "reasonable" expectations are fulfilled?

MR. GREENAWALT: I think it's a combination of both. That is, I think it's ultimately a normative question.

MR. BLAKEY: What is the criterion for the normative judgment?

CHAIRMAN ERICKSON: What he is saying and what I have been watching him lead up to in a hundred different directions is to get you to draw the line. That is the point that I think he is getting ready to ask.

MR. GREENAWALT: To some extent, because we are the product of the expectations that we have had, when you deprive people of expectations which they now have, that may be more serious than keeping deprivations of privacies that they might have but which they don't now have.

So I think the normative question as to what kinds of expectations you want to protect depends

in part on what expectations people now have. But they are distinguishable questions. They may have some expectations you don't think they should have, and they may not have some expectations you think they should have.

MR. BLAKEY: So the normative issue is the real one?

MR. GREENAWALT: But I think the empirical question of what people do expect is relevant.

MR. BLAKEY: What are the criteria for the normative judgment?

MR. GREENAWALT: I think now you are pushed into the general theories of privacy, the kind of thing Professor Westin has written about, and so on. Do you really want to go into those?

I suppose one is in terms of the impact on the personality of the person whose privacy is being intruded upon. You look to see what the general effects on social institutions will be if certain kinds of privacies are observed or not observed, and so on. I think you have to go into a very intricate analysis, including utilitarian purposes of privacy, the moral value of privacy, and so on.

MR. BLAKEY: And evaluate it against the need of law enforcement, which are also the needs of society?

MR. GREENAWALT: Yes.

MR. BLAKEY: Thank you, Professor.

CHAIRMAN ERICKSON: Chief Andersen.

MR. ANDERSEN: Mr. Blakey has asked you about telephonic search warrants. We have it in two states now, Arizona and California. I was going to ask on the emergency concept about a plain telephonic warrant. I am looking to Arizona or California where you can get search warrants by a phone call to the judge, and then file it 24 hours later or 48 hours later, or something.

MR. GREENAWALT: Of course, as far as *Katz* is concerned, there is a suggestion in the opinion that no emergency surveillance is legitimate under the Constitution. This, I guess, would avoid that if the judge got enough information so that he could form a judgment meeting ordinary standards of probable cause.

I am a little hesitant to think that when a judge talks over the phone he can make the kind of considered judgment we'd like to think should be made by judges issuing warrants, although I think usually judges usually don't make that kind of judgment when they issue warrants.

With that kind of reservation, I think it would be a preferable procedure to authorizing emergency surveillance without judicial approval.

MR. ANDERSEN: In a broad area, in your White House Office of Telecommunications, you apparently look at these policies of telecommunica-

tions. I don't know if this should be part of Title III. But have you given any consideration about the overhearing of digital communications, macrowave computer links, and that sort of communication, and what its relation is to Title III, if any?

MR. GREENAWALT: I mentioned that in the report and I drew from the seven pages of Arthur Miller's book which discussed that. I found his analysis to be persuasive. What he says is that the apparent language of the statute doesn't cover digital communications and he sees no reason why it shouldn't be covered by the statute. That seems to me to be sensible.

MR. ANDERSEN: Do you think we should give consideration, in this review under Title III, to the concept of literally tapping computer links and that type of communication?

MR. GREENAWALT: I don't know what your priorities are in terms of other problems. I don't think that is the greatest problem about wire-tapping, and I'm not in a position to say that is so important that you should spend more time on it if that means spending less time on other problems, but I think it is important enough so something should be done about it.

MR. ANDERSEN: Then on the tapping of "information," your feeling is on the privacy of conversations between people and not the privacy of the contents?

MR. GREENAWALT: You mean in suggesting that maybe digital transmissions are not so important I am impliedly saying that?

MR. ANDERSEN: I guess—

MR. GREENAWALT: Let me take it back, then. I think if these do involve personal information, which they must, because some of that information is on quite a few computers, then I would think it would be a matter of major importance and definitely should be considered by you.

In other words, I think that wiretapping is a serious threat not only because a conversation is going on between two people but because important information about those people is passed.

MR. ANDERSEN: And we will have access to your report? Will it have some data on that in it?

MR. GREENAWALT: I think almost everything I said is in the 30 pages I submitted.

MR. ANDERSEN: I have no further questions.

CHAIRMAN ERICKSON: Judge Shientag.

MS. SHIENTAG: Professor Greenawalt, I am troubled by your statement that a more important reform would be the number of authorities issued for eavesdrop orders, and you say that virtually no applications to eavesdrop have been turned down. Do you recall making that statement?

MR. GREENAWALT: I do recall making that statement.

MS. SHIENTAG: Are you aware of how many administrative levels there are—and I assume you are because you were in the Solicitor General's Office—between the time an FBI agent, for example, seeks an order, and the time he gets the approval of the Attorney General?

MR. GREENAWALT: I am aware of that.

MS. SHIENTAG: And isn't it about ten levels?

MR. GREENAWALT: Well, I never counted them, but certainly there is extensive review.

MS. SHIENTAG: We have had testimony to that effect that it goes from him to the special agent in charge, and then it goes down to the FBI Bureau where it is reviewed several times. It is referred to the Department of Justice where it goes through periods of review, and finally reaches the Attorney General or his specially designated deputy.

MR. GREENAWALT: I think the specially designated Assistant Attorney General, actually.

MS. SHIENTAG: Assistant, yes.

Now, couldn't that be the reason why virtually no applications to eavesdrop have been turned down, because there has been such a scrutiny before the request goes to the court?

MR. GREENAWALT: That certainly is a possibility, and my belief on relatively little knowledge is that the scrutiny was very careful in the Justice Department.

I think I'd make two comments about that, though. First of all, there isn't any provision for such careful review in regard to state eavesdrop applications.

And second, the experience with search warrants—not eavesdrop warrants but just general search warrants—is that judges tend to issue them pretty much on a rubber-stamp basis, and that certainly if law enforcement authorities can find judges who are favorable, they will be able to find a judge who will approve virtually any application they want to give him.

So that led me to think that even if there were less careful review in the Justice Department, it would probably still be true that not many eavesdrop applications would have been refused.

But yours certainly is one possible explanation for the present fact that as far as Federal applications are concerned, few have been refused.

CHAIRMAN ERICKSON: Just a few questions.

Of course as to the rubber-stamp argument that you hear so much about on the search warrants, the police are the ones who suffer if they follow that procedure because appellate courts have a tendency to follow *Spinelli* and *Aguilar* and because all those search warrants that are the product of the rubber stamp fall.

MR. GREENAWALT: That certainly is right, and I suppose it is the fear that will happen that will make the law enforcement officers much more careful in getting warrants.

CHAIRMAN ERICKSON: So it is a disservice to them if the judge does that?

MR. GREENAWALT: Yes, it is.

CHAIRMAN ERICKSON: In *Giordano*, the result of not complying with the statute was that a number of convictions fell.

MR. GREENAWALT: Yes, that is right.

CHAIRMAN ERICKSON: So we get down to the point that we have a statute that has to be construed very carefully just as you construe a search warrant. In your opinion is the emergency provision practical, because of all the steps of review that you have to go through, to either an Assistant Attorney General or to the Attorney General himself?

MR. GREENAWALT: Yes. Again, I think that is right, that if there is an emergency need it would make sense to allow a temporary approval of the application for the order by some lower Federal officer.

CHAIRMAN ERICKSON: And have a procedure that might come closer to meeting constitutional scrutiny?

MR. GREENAWALT: Yes. Again, of course, there aren't such lengthy procedures built in for state applications for eavesdropping.

CHAIRMAN ERICKSON: The expectation of privacy is what we are really talking about, isn't it? If you stand on a soap box in Madison Square Garden and describe your plans to burglarize the Biltmore, you certainly can't complain if a police officer standing in the front row records everything that you say; isn't that correct?

MR. GREENAWALT: On that state of facts, I would agree with that.

CHAIRMAN ERICKSON: And if you are in your lawyer's office discussing what you have done with him, you have a right to expect that that is going to be private.

MR. GREENAWALT: Yes.

CHAIRMAN ERICKSON: And if you are in your bedroom telling your wife what you have done, you can again expect privacy?

MR. GREENAWALT: Yes.

CHAIRMAN ERICKSON: If you are, on the other hand, talking on a party telephone line, you have no reason to expect privacy, particularly when some little girl wants to call her girlfriend and is coming on and over the line saying, "Get off the phone; get off the phone." You wouldn't have any reason to expect privacy under those circumstances?

MR. GREENAWALT: Here I'm going to disagree with you.

CHAIRMAN ERICKSON: I am getting to the point where I ask you to draw the line. Where do you expect privacy? I asked General Clark about the jail cell. If you talk to a person in a jail cell, do you have a right to expect that he will keep in confidence what you tell him or that it won't be overheard?

MR. GREENAWALT: I tend to agree with him that that is a situation in which society should provide some expectations of privacy.

CHAIRMAN ERICKSON: How about *Miller v. California*, which really put a crimp in *Massiah*, where the woman had done away with her husband and run away with her paramour, and described her entire escapade to a police officer that was incognito in the jail cell with her. And she already had counsel, so we had *Massiah* squarely in operation. The Supreme Court of the United States dismissed certiorari and said, "There is no expectation of privacy in a jail cell."

MR. GREENAWALT: I'd like to back up a little bit. You asked me if there is an expectation of privacy. One question is where the court is going to draw the line as a matter of constitutional law? Another question is where you are going to draw the line in terms of what you are going to recommend?

CHAIRMAN ERICKSON: If we are going to recommend that this statute be used to protect privacy, we have to look at what privacy the act is intended to protect.

MR. GREENAWALT: Well, the only point I'd like to make now is that I think in the jail situation where somebody is incognito, in the ordinary situation in which an informer is used for law enforcement purposes, in the situation where there is a recording system like President Nixon's, we do have expectations of privacy when we are talking to another person, even if nobody from outside is interfering.

CHAIRMAN ERICKSON: In your testimony here, it is being recorded by the court reporter.

MR. GREENAWALT: Well, I have no expectation of privacy about that because I know that it is happening.

CHAIRMAN ERICKSON: When you were up here talking to me before you testified and we went through this emergency procedure and you repeated it here, did you have reason to expect that that conversation would be private? No one else was around.

MR. GREENAWALT: No, but that is only because of what we were talking about. We were talking about this subject matter, and I think the normal human expectation is that you would feel perfectly free if I had said anything that I hadn't

said in testimony that you wanted to pass on—that you'd be perfectly free to pass that on to anybody who is interested in the subject.

But if you had asked me how did I feel today and I said, "Oh, I feel terrible. I had a terrible argument with my wife last night and we had too much too drink," then I think I would expect you not to relay that to other people, and I would have an expectation of privacy.

CHAIRMAN ERICKSON: We are in a jail cell together and you tell me that you want me to help you break out of jail. And of course, the purpose of jail is to keep you there so the warden of the jail or the jailer has a reason to try to protect against any conspiracy to get out of the jail. Shouldn't he be able to surveil the conversations that would be conducted for the purpose of conducting a jail break?

MR. GREENAWALT: That is a question of balancing society's interest in keeping secure jails versus the ordinary interests and expectations of privacy, I think.

But unless you think that it would be acceptable to have the kind of prison that people's homes were in the novel *1984*, where everything that was done in the home was overheard—an obvious bug on every cell so everybody knew they never could say anything which somebody else wouldn't overhear—unless you accepted that kind of situation, I would say in this situation the prisoner does have some expectation of privacy. I would think it an expectation of privacy that is of some social value. Then I think you get into the balancing process as to whether the need of the warden to hear these kinds of conversations outweighs the need of the prisoner to have some privacy. But I have no doubt there is an expectation of privacy that is being destroyed in that situation.

The preliminary part of my report which I have not given you does go into some of these theoretical things in some more detail.

CHAIRMAN ERICKSON: You are familiar with the report that has been filed with the Administrative Office, the one that is filed annually. Have you examined those reports?

MR. GREENAWALT: I have not examined them, no. I read Professor Schwartz' examination of the reports, and I have read some other things about the reports, but I never sat down and read the reports.

CHAIRMAN ERICKSON: I was just going to ask you if you thought the report carried out the functions of the statute or whether or not the reporting requirements ought to be amended to require more specificity.

MR. GREENAWALT: I have some reaction from the articles that I have read, but I am really not in a position to answer that.

CHAIRMAN ERICKSON: I have no further questions.

Do any other members of the Commission have questions before I extend the grateful thanks of the Commission for your testimony and for the learned writing that you have provided us and for the writing that you are yet to provide us that will be used in the final report?

Thank you very much for coming, and we hope we haven't delayed you too long.

MR. GREENAWALT: Not at all. Thank you very much, Mr. Chairman.

[The document referred to follows.]

Excerpts From Report on Privacy—Its Meaning
and
Legal Protection
by Kent Greenawalt

b. *Electronic Surveillance*

Before 1967, wiretapping and electronic bugging that did not involve some physical intrusion on premises were considered not covered by the Fourth Amendment. Section 605 of the Communications Act of 1934 forbade interception and divulgence of telephone and radio messages. The Justice Department defended government wiretapping on the debatable theory that only interception and divulgence were prohibited and that communication between government officials was not divulgence.

A new era of regulation of electronic surveillance was ushered in in 1967 and 1968, with sweeping changes in constitutional doctrine and legislative regulation. The Supreme Court decided in *Berger v. New York*, 388 U.S. 41 (1967), and *Katz v. United States*, 389 U.S. 347 (1967), that wiretapping and electronic bugging were reached by the Fourth Amendment even in the absence of any physical intrusion, and that the traditional requirements of the Fourth Amendment were applicable, including court approval before surveillance is carried out. More recently, the Court rejected the Administration's position that electronic surveillance of domestic "subversives" could be carried out without court orders, *United States v. U.S. District Court*, 407 U.S. 297 (1972), but it has yet to decide whether court orders must be obtained for surveillance relating to the activities of foreign powers.

Congress passed systematic legislation on eavesdropping as part of the Omnibus Crime Control and Safe Streets Act of 1968. Title III of that act is a comprehensive approach to electronic eavesdropping, 18 U.S.C. Sections 2510-2520. Private wiretapping and private bugging with electronic devices are prohibited. The statute creates a civil damage action that includes liquidated damages, punitive damages and an allowance for attorney's fees and other costs of litigation. Despite these generous encouragements to civil recovery, however, few suits have been brought under the act.

The act permits law enforcement eavesdropping under a court order system. With respect to a fairly broad class of criminal offenses, including, for example, all drug offenses and gambling, eavesdropping can be approved by a federal or state court order.

Whether wiretapping and bugging should be allowed at all in ordinary criminal cases will no doubt be the subject of recurrent debate, and many states continue to prohibit it. The net of electronic surveillance catches innocent as well as criminal conversations, and it catches the conversations of all those who speak with the subject of the eavesdropping. When some electronic

eavesdropping is legal and the relevant devices for surreptitious overhearing are available, the likelihood of unauthorized eavesdropping is considerably increased. For these and other reasons some critics will continue to believe that the sacrifice in individual privacy from legalized electronic surveillance is too great to justify the benefits to law enforcement. See, for example, Final Report on Privacy in a Free Society of the Annual Chief Justice Earl Warren Conference sponsored by the Roscoe Pound-American Trial Lawyers Foundation (Cambridge, Mass.) 1974. Even if one accepts the need for some eavesdropping, the act is still subject to attack for permitting too many persons to obtain orders in too many courts for too many offenses and for too long a time.*

The act provides for a National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance. It has now been appointed and is reviewing the effectiveness of the act. Its conclusions will be based on a detailed study of the act's operation in practice. Regrettably, the evidence about electronic surveillance has always been ambiguous; and even were there agreement on factual conclusions, conflicts over the importance of various interests would lead to divergent evaluations of the law's proper scope. We may hope that the Commission can provide a firmer factual footing for evaluation, but it would be exceptionally optimistic to expect better understanding of relevant facts to lead to consensus about the appropriate reach of electronic surveillance. An examination of the Commission's operational plan suggests that it will probably not make a sweeping assessment of the desirability of law enforcement eavesdropping, although it may well come up with some proposed modifications in present legislation. Because the Commission's work may permit more accurate evaluation of the act and because wiretapping and eavesdropping are not yet primary concerns of the Committee on Privacy and the Office of Telecommunications Policy, I do not undertake a systematic assessment of the act's provisions. Since the proper extent of law enforcement eavesdropping is a very important subject for those concerned with privacy, however, I do sketch in a preliminary manner what seem to me to be defects in the present act.

The act permits electronic surveillance for far too many crimes. Section 2516 allows authorizations not only for such serious federal crimes as sabotage, treason, murder, kidnapping, bribery, and obstruction of justice, but also for crossing state lines with intent to commit a riot, gambling offenses, and any offense of dealing in heroin, marijuana, or other dangerous drugs. State orders may be granted for all gambling and drug offenses, as well as more serious crimes, and for any crime "dangerous to life, limb, or property, and punishable by imprisonment for more than a year." This last provision is simply a surrender to the states to decide how extensive they want eavesdropping to be, and is really inconsistent with the notion of a restricted class of crimes. Since many telephone calls are interstate and many other conversations cover interstate matters, and since law enforcement eavesdropping touches important federal constitutional rights, checking unjustified eavesdropping is a problem of national concern, and Congress has abdicated its proper responsibilities in leaving the states such latitude.

Wiretapping and bugging are relatively expensive means of law enforcement. See H. Schwartz, *Reflections on Six Years of Legitimated Electronic Surveillance*, supra, at 47-48. A majority of states have still not passed the enabling legislation necessary under the federal act to allow their law enforcement officers to eavesdrop; and the great preponderance of state authorized

* See Federal Legislation and Civil Rights Committee of Bar Association of the City of New York, *Proposed Legislation on Wiretapping and Eavesdropping*, Reports Concerned with Federal Legislation, Vol. 7, Bull. No. 2, Aug. 1968, p. 1; H. Schwartz, *The Legitimation of Electronic Eavesdropping: The Politics of "Law and Order,"* 67 Mich. L. Rev. 455 (1964); H. Schwartz, *Reflections on Six Years of Legitimated Electronic Surveillance*, in *Final Report on Privacy in a Free Society*, supra, at 38.

eavesdropping takes place in two states, New York and New Jersey, *id.* at 48. If most states can do without eavesdropping altogether and others can do with relatively little, then certainly there is no need to authorize it for such a broad range of state offenses.

One possibility would be to reserve eavesdropping for crimes of the utmost gravity, like murder and kidnapping, though the statistics of the past few years have confirmed the common assumption that only in very rare instances is eavesdropping valuable in the solution of these crimes. There is, however, a special argument for eavesdropping on gambling and drug offenses. Eavesdropping is thought particularly useful against organized criminal activities, and the grist of these activities is crimes of vice, like narcotics, gambling, and prostitution. Surveillance may reach the conversations of "higher ups," or it may provide irrefutable evidence against lower level figures who can then be persuaded to trade their testimony against their bosses for leniency from law enforcement officials. Another argument for wiretapping on gambling activities is that often particular telephones are used exclusively for gambling and that interception, therefore, does not intrude upon innocent conversations. Apparently law enforcement officials have not limited themselves to organized gambling and drug offenses, but also eavesdrop on "small-time operators." It would be very difficult to draft appropriate language limiting eavesdropping to gambling and drug offenses of large magnitude or committed by participants in organized crime, although law enforcement agencies could limit eavesdropping to those circumstances. A statute could forbid authorization of eavesdropping to discover gambling in situations in which many innocent conversations are likely to be overheard. Whatever is done about gambling and drug offenses, the statute should be revised to forbid eavesdropping for crimes which are neither especially serious nor have some special connection to more serious crimes.

Every eavesdrop order must state the period of time of authorization, indicating whether or not the surveillance shall automatically terminate when the described communication has first been obtained. This language was intended to meet the Supreme Court's criticism of a New York statute that placed no termination date on eavesdrops. But since judges need not provide automatic termination if the application shows that further conversations are expected, the police will still be able to continue surveillance in cases when that would be useful. The maximum length for authorized eavesdropping is 30 days, but renewals may be obtained for subsequent 30-day periods if a new showing of need is made of the kind necessary for an initial authorization. The statute contains no absolute limit on the length of particular surveillance, and if continuing criminal activity is taking place, each renewal application in turn may be able to demonstrate the need for further surveillance.

It is certainly questionable whether any surveillance should be allowed for as long as thirty days. Unless a telephone is used exclusively for criminal activities, vast numbers of innocent conversations are bound to be swept up. Perhaps there are rare situations of the utmost urgency when a long surveillance is essential, not only to gather extra evidence or catch peripheral participants, but to ascertain key participants and get vital evidence against them. One statutory approach would be to set an ordinary limit of a few days for electronic surveillance, but to permit longer surveillance if the risk of intercepting innocent conversations was very low, as with the telephone used exclusively for gambling, or the public need for continued surveillance was very great, judged in terms of the seriousness of the crime and the importance of further surveillance to solve it.

As my comments thus far have implied, perhaps a statute should contain an explicit balancing test, requiring a judge to weigh carefully the seriousness of the crime and the likelihood of overhearing innocent conversations in deciding whether to authorize any surveillance at all and in determining the length of

permissible surveillance. The act does already require a showing that other law enforcement techniques are not likely to succeed or are too dangerous, §2518(3)(c). While this salutary preference for other methods may have some effect on law enforcement agencies, a judge is not in a very good position to reject assertions that other techniques will be ineffective or dangerous; and it is hard to see how more teeth could be put into the existing provision.

The existing act draws no distinction between wiretapping and bugging. Bugging is usually a much more pervasive invasion of privacy. Since a bug may pick up all conversations in a room in one's home or in one's office, it will almost surely intercept many innocent conversations and it intrudes upon areas felt to be especially private. Whatever restraints are placed on overhearing of telephone conversations, even more severe restraints are warranted in respect to conversations within the confines of one's home or office. As far as telephone conversations are concerned, the present statute does not apparently regulate police listening at extension telephones or private switchboards. In the absence of consent by one of the parties to a conversation, such listening should be made subject to the act's requirements.

There are some special restraints on authorization of eavesdropping in the present statute. Either the Attorney General or a specially designated Assistant Attorney General must approve federal applications, and state applications must be authorized by the principal prosecuting attorney of the state or of one of its subdivisions. The federal limitation here seems appropriately narrow, though inadvertent failure to observe the statutory guidelines within the Justice Department has resulted in the invalidation of probably hundreds of eavesdrop orders over a period of years because neither Attorney General Mitchell nor an Assistant Attorney General actually approved the applications. The statute can be criticized for allowing the principal prosecuting attorneys of small political subdivisions to authorize eavesdrop applications. One possible way of assuring the importance of eavesdrop requests would be to channel all of them through the federal government, though the centralization of power this procedure would involve might raise objections. A more important reform would be sharply to limit the number of courts authorized to issue eavesdrop orders. Presently law enforcement officials may "shop" for sympathetic state and federal judges and virtually no applications to eavesdrop have been turned down. Allowing only a relatively small number of designated federal judges to issue orders would tighten the authorization procedure in a useful way.

One of its most controversial provisions is the act's authorization in some circumstances of emergency surveillance without a court order for up to two days. § 2518(7). Law enforcement officers have wisely made little use of it. In *Katz v. United States* the Court spoke of a court order as a "constitutional precondition" for electronic surveillance, and cast very serious doubt on whether any emergency could justify surveillance without such an order. Since it typically takes time to set up surveillance, and, especially in large cities where most surveillance takes place, magistrates can usually be reached within a few hours, there is no persuasive argument for emergency power. It might be argued that such power does little harm because after 48 hours a judge must pass on the surveillance in any event, but this argument omits the danger that the police may violate the act by eavesdropping briefly on less than probable cause in the hope of picking something up. If they are successful, they can construct a case that probable cause existed in the first instance, and it will be hard for a judge to find it lacking if evidence of crime has already been uncovered. If the eavesdropping fails, the police may disregard the act's requirement that they apply to a judge, since no one else will know the eavesdropping has occurred. Even if this emergency power were not given, there would be danger of unauthorized surveillance and of fabrications of probable cause, but the dangers in connection with the emergency power are so

apparent and the need for the power so slight, it was plainly a mistake to attempt to give such power, and that power should be taken away.

Within 90 days of the end of any surveillance or the denial of an application for surveillance, the persons named in the order are to be served with an inventory informing them of the order or application, the period of authorized interception, if any, and whether or not communications were intercepted. § 2518(8)(d). Other parties to interceptions are served with a similar inventory if the judge determines "in his discretion that (it) is in the interest of justice." An inventory may be postponed, apparently without limit, upon a showing of good cause by the government. Upon motion by the person served with an inventory, the judge may in his discretion make available for inspection "such portions of the intercepted communications, applications and orders as (he) determines to be in the interest of justice." If evidence of an intercepted communication is to be presented in a trial or other proceeding, then each party must be served with a copy of the authorizing order and application.

These apparently technical rules are of considerable importance. The first point to notice is that even the person against whom surveillance is directed has no absolute right to see either the order or the application, unless intercepted communications are to be used in evidence against him. If the surveillance was not based on probable cause or is otherwise defective he has suffered a violation of his rights under the statute and may be entitled to recover civil damages as a consequence (an official's good faith reliance on a court order is a defense to a civil claim but an officer who lied to establish probable cause would certainly be liable). What is more, invalid surveillance will usually violate constitutional rights as well as statutory ones. The person subject to surveillance is in no real position to judge its legality unless he sees the application and order, and he should be served with these as a matter of course, unless perhaps a specific showing is made of confidential information that should not be disclosed. Nor does there seem any good reason not to let the person subject to surveillance have the record of his own intercepted communications if he wishes them. The statute provides that these are to be recorded, if possible, so the problem is not one of availability. An inventory after an ordinary search would clearly enumerate what has been seized. If a person can not recall his conversations, there would seem to be no reason to deny him information in the government's hands. Conceivably if some of the conversations relate to crime, knowing exactly what is said will help a criminal repair damage, but is much more important that persons be able to know the precise intrusions on their privacy and to be as aware as possible of the bases for potential misuse of information in the hands of the police. Nor, if one regards electronic surveillance as seriously intrusive of privacy, will the expense and inconvenience of furnishing the conversations be a substantial argument against doing so. Again, if there is to be any exception to furnishing the conversations themselves on demand, it should be narrowly formulated to respond to very specific and powerful reasons for withholding.

At least the person named in the order is ordinarily in a position to assert his interest in getting the order, application, and conversations. But other parties to conversations do not even receive inventories as a matter of course, and will probably never find out that their conversations were intercepted unless the main subject of surveillance tells them. It is hard to know how a judge is supposed to exercise his discretion to decide if others will receive inventories, but the way the statute is drafted the presumption seems to be against any general serving of inventories. This does conform with ordinary search and seizure practice; only one inventory is typically serviced though others (guests in the house or persons whose property is in a house) may have their constitutional rights affected. However, in the area of electronic surveillance, the intrusion on the privacy of others is much more typical. Their rights under the statute and

constitution are violated by illegal surveillance, and they can not possibly take action if they do not know the intrusion has taken place. Now that the Supreme Court has established an independent right to recover for constitutional violations the argument is much stronger than it used to be that persons whose constitutional rights may have been violated should be told of this even if they have suffered no injury under ordinary tort principles.

There is also a more substantial issue of policy at stake. If innocent people are rarely informed when their conversations are intercepted, they have little basis to evaluate the degree of intrusion on privacy that surveillance entails. If inventories were served on all persons whose conversations were overheard and who had been identified by law enforcement officers, this would no doubt be burdensome, but it probably would give people some better way to determine if the gains of surveillance are worth the price. We can suspect that such inventories, followed by access to the intercepted conversations themselves, would generate considerably broader concern over eavesdropping, and this may be one reason why law enforcement officials would prefer not to serve them. Serving inventories more broadly, especially if affidavits and authorizing orders were also provided, might have the adverse effect of giving friends and business associates a basis for suspecting each other of unproved crimes and might even lead to another set of government records of suspected people, but this cost might be worth the benefit of giving the public a fuller idea of the incidence of surveillance.

Some provision for postponement of an inventory is sensible since the evidence obtained from surveillance may be employed in further investigation, but the reference to "good cause" in the statute and the absence of any terminal date for a postponement leave the provision too open-ended.

My comments on possible reform of specific defects in the present statute should not be taken as implying that a statute corrected along these lines would be preferable to a ban on ordinary law enforcement eavesdropping. I am not yet persuaded that the gains from eavesdropping under any authorization system would outweigh the costs, but if eavesdropping is to be allowed, it should be under stricter constraints than now exist.

There are four special issues about eavesdropping and the present legislation to which the National Commission does not plan to devote substantial attention. The best known of these is the proper treatment of national security surveillance. The Supreme Court has not yet resolved whether surveillance of the activities of foreign powers may constitutionally be carried out without court orders. If there is to be an exception to the court order requirement, it is unclear how extensive it will be. Finally, *United States v. United States District Court*, 407 U.S. 297 (1972), leaves open the extent to which ordinary probable cause and particularity standards might be relaxed when the government seeks court orders for domestic security surveillance. The same question of possible relaxation would arise for whatever surveillance of foreign activities is held to be subject to court order requirements.

Congress has made no effort to set standards on these subjects, nor has the Administration announced guidelines. The 1968 act, 18 U.S.C. § 2511(3), does specifically provide that no limitation is intended of the President's power to protect the nation against attack, to obtain foreign intelligence information, to protect national security information against foreign intelligence activities, and to protect the government against overthrow or other clear and present dangers. The act does not state the extent of Presidential powers; it simply refrains from limitation of whatever powers exist. The Supreme Court has established that surveillance of a purely domestic group requires a court order, but its decision leaves open the constitutional need for a court order to precede eavesdropping directed at the following kinds of targets: foreign embassies and consulates; aliens suspected of engaging in military and political intelligence work for their countries; aliens suspected of engaging in economic intelligence;

aliens whose conversations may reveal military political, or economic information about foreign countries; American nationals dealing with foreign governments; American nationals who may know important facts about foreign countries; American groups enjoying some foreign support; American groups (like the Jewish Defense League) whose activities may have foreign repercussions; American nationals who may reveal to other nationals information that may subsequently find its way to foreign governments (the members of Dr. Kissinger's staff who were the subjects of wiretaps were thought by those approving the wiretaps possibly to fit in this last category). It is easy to see that if the court order requirement were waived whenever an activity had any connection, however remote, with the activities of foreign governments and with United States national security, broadly defined, then there would indeed be large classes of exceptions to court order standards. If the Supreme Court creates any exceptions, they will presumably be narrower, but it is impossible to know precisely how they will be formulated. Obviously as the target of the eavesdropping becomes more domestic, as the connection with foreign activity becomes more remote, and as the security importance of the activity diminishes, the argument for warrantless surveillance weakens.

Since Congress is free to require court orders and the Administration is free to refrain from warrantless surveillance even in situations when such surveillance is constitutionally permissible, it would make sense for the legislative and executive branches to develop appropriate standards, especially since the Supreme Court is unlikely to settle all the relevant issues at one time.

I do not find the argument against court orders to be very persuasive. See Note, "Foreign Security Surveillance and the Fourth Amendment," 87 *Harv. L. Rev.* 976 (1974). Hearings on applications can be held *in camera*, the government being able to choose from which judges to seek authorization. It is really not believable that there are many matters that are so sensitive knowledge of them can not be trusted to a single federal judge of the government's choosing, especially since judges are now sometimes placed in the position of reviewing the legality of surveillance retrospectively when defendants claim they have been subjected to illegal eavesdropping. If court review in advance is tolerable, it may still be doubted if it is likely to be effective. Judges may be ready to sustain almost any government claim that surveillance is required for national security. Nonetheless, requiring the government to make out a case will itself impose some restraint. Surely one of the lessons of the last few years, and of less recent history, is that those responsible for protecting national security often see or claim to see threats where no detached observer could find them. A court order system would be one safeguard against paranoia or disingenuous assertions of dangers to the country.

If Congress is persuaded, contrary to the gist of the last paragraph, that court orders should not always be required, then it should circumscribe as carefully as possible exactly the kinds of situations in which the government should be able to engage in warrantless surveillance.

The proper standards for surveillance pose, in my view, a much more difficult issue than judicial review. One can imagine circumstances when continual surveillance is justified or possible threats to the country so grave that surveillance of a particular subject should be allowed even when the likelihood that it will produce helpful information is fairly slight. If, for example, there were a reasonably founded fear that country X planned a first strike of nuclear weapons, lengthy surveillance of those who might conceivably reveal relevant information would be warranted. However, if relaxed standards are sometimes appropriate, they are not appropriate for every tenuous connection to some foreign activity touching indirectly the security of the country. The government should not be able to eavesdrop on a Japanese car maker visiting in the country because the future

prices of Japanese cars will affect our domestic economy and our relations with Japan. At this stage in history, I am doubtful that electronic eavesdropping of American nationals whose activities are unconnected to foreign activities should ever be justified on "relaxed" standards. Thus, I think Congress has rightly not tried to write into the statute a separate court order system for domestic subversion. But a careful Congressional delineation of the bases for eavesdropping in foreign security matters would be very useful. A tightly drawn statute would permit surveillance on a lesser showing and for longer periods in respect to foreign activities that have an intense impact on national security, but "national security" would not become a label to justify abandonment of ordinary protections on tenuous or artificially constructed grounds.

The second general issue the National Commission apparently will not address is much more technical, the apparent inapplicability of the statute to digital transmissions made from one computer to another. See §2510. The statute protects wire and oral communications from interception. Without a great stretch in ordinary language, digital transmissions could not be called "oral communications." If carried over the facilities of common carriers, they do seem to meet the act's definition for wire communications, but what the act forbids is interception of such communications and "intercept" is defined as "the aural acquisition of the contents of any wire or aural communication." Again, interception of a digital transmission would not be an "aural acquisition" in any ordinary sense. There seems no good reason to withhold protection from digital transmissions, and amendments to this statute may be the most sensible way to safeguard them. See Arthur R. Miller, *The Assault on Privacy* (Ann Arbor: Univ. of Mich. Pr. 1971) pp. 161-168. In any event, this is obviously a problem that merits the careful consideration of executive agencies and legislative committees.

Another crucial question, touched on below in more detail, is what protection should be given to other parties when one party to a conversation records or transmits the conversation without their knowledge, or allows someone else to listen with an electronic device. The present statute does not touch such action by public officers and prohibits it when engaged in by private persons only if they are trying to commit a crime, tort, or other injurious act, 18 U.S.C. Section 2511 (2)(c) and (d). I am aware of no cases arising out of this prohibition. Whether greater protection should be given against "participant monitoring" is one of the most heated issues concerning eavesdropping. Since the Commission apparently plans only to consider whether consensual eavesdropping should be reported under the act's disclosure provisions, debate about extending the act's prohibitions should not await the Commission's findings.

A fourth issue is of somewhat lesser importance, whether the act should be extended to "pen registers" and methods used to trace telephone calls. If one merely ascertains the outgoing number dialed on a telephone by a pen register, he does not acquire "the contents" of a communication. Therefore, the restrictions of the act presumably are inapplicable though court orders for pen registers have sometimes been sought. See *United States v. Giordano*, 416 U.S. 505 (1974). There may be arguments that law enforcement discovery of numbers called should be subject to less rigorous safeguards than interception of the conversations themselves, but, absent some strong social interest to the contrary, whom we talk to on the telephone should be as confidential as what we say. At the very least most private attempts to determine by electronic device who is calling whom should be forbidden as they were under Section 605 of the 1934 Communications Act . . .

e. *Participant Monitoring With Electronic Devices*

Frequently one party to a conversation uses electronic means to record or transmit the conversation without the knowledge of the other parties. Or he may consent to an outsider's using an electronic device to overhear the conversation. In many settings electronic equipment is used to assure an accurate account of a conversation in which an informer is involved. In other settings someone who is not an informer in any ordinary sense, such as the parents of a child that has been kidnapped or the victim of extortion, may wish to have the police hear what is being said. In still other settings, such as the recording system in the Nixon White House, one party to a conversation may wish an accurate record for possible future use, but with no intent to damage the other parties to a conversation and with no intent even to disclose the conversation more broadly in the near future.

Is any intrusion on privacy involved in those practices? At the least there is a subtle alteration in the conditions of the conversation unknown to one of the participants. Even when the person making a recording does not intend to harm the other participant or disclose more broadly what he has said, the other participant might choose his words more carefully or even refrain from expressing some ideas if he knew what he was saying was being reproduced in semi-permanent form. Indeed these are the very reasons why the person making the recording may not wish to tell the other person about it.

An informer or secret agent is already deceiving the other participant about the conditions of a conversation. What does the electronic transmission or recording add to the intrusion upon privacy? It assures that there will be a complete and accurate account of what has been said, and evidence beyond the informer's word that the conversation has taken place. When we speak confidentially we may often rely in part on the evanescence of words and the ability to claim that we have been misquoted or misunderstood if the person to whom we talk does disclose more broadly than we wish. The presence of a recording or transmitting device eliminates this protection of limited dissemination, and thus does pose an added threat to privacy beyond the presence of the informer himself. See generally, K. Greenawalt, "The Consent Problem in Wiretapping and Eavesdropping: Surreptitious Monitoring with the Consent of a Participant in a Conversation," 68 *Colum. L. Rev.* 189 (1968). The ease with which tape recordings apparently can be "doctored" and the difficulty of proving that this has happened magnify the threat of recordings to communication; for the unwitting speaker may even have "reproduced" as accurate remarks that in fact he never made or made in quite a different context from that appearing on the tapes.

Whenever it has faced the question squarely, the Supreme Court has held, most recently by a 5-4 margin in *United States v. White*, 401 U.S. 475 (1971), that no constitutional problem is presented if an informer or government official records or transmits a conversation unknown to the other party to a conversation.

As mentioned above, the federal eavesdropping statute does reach a very limited number of instances in which a party to a conversation transmits or records it. Some state laws go further and forbid all participant monitoring. In 1966 the Federal Communications Commission prohibited the private use of radio devices to monitor conversations in the absence of consent of all parties to the conversation, 31 Fed. Reg. 3397, but the penalties were not terrifying, a fine of \$500, loss of license, and civil forfeiture. The 1968 act on wiretapping and eavesdropping apparently did not supplant this regulation, but the regulation has been enforced very little or not at all.

In *Rathbun v. United States*, 355 U.S. 107 (1957), the Supreme Court decided that Section 605 of the Communications Act of 1934 did not forbid one person from allowing another to listen at an extension telephone without the knowledge or consent of the other party to the conversation. Given the frequency with which parties to conversations allow family members or em-

ployees to listen on extension telephones and the severity of Section 605's penal sanctions, the Court concluded that it would be unreasonable to suppose that Congress meant to proscribe such listening. Apparently under the 1968 act, a party might even allow another person to place a wiretap on his telephone to intercept a conversation, so long as the purpose of the wiretap were not to commit a crime, tort, or other injurious act. Certainly the rule that one may permit use of his extension phone stands. As to surreptitious recording of conversations, however, a special Federal Communications Commission rule is applicable. That requires telephone companies to assure that any use of recording devices in interstate and foreign calls be accompanied by an automatic "beep-tone" supposed to warn the other user his words are being recorded. See *In re Use of Recording Devices in Connection with Telephone Service*, 11 F.C.C. 1033 (1947). The companies in turn include such a "beep-tone" requirement in their tariffs for users. Many state commissions and companies have similar requirements for local calls. Violation of the Commission's rule by a company can result in a fine of \$500 per day; apparently the only sanction against the individual user is possible loss of telephone imposed by the company. In light of the difficulty of discovering violations and the rather pitiful sanctions, it is hardly surprising that the "beep-tone" requirement is frequently disregarded.

At the narrowest level, the problem might be seen as effective enforcement of the "beep-tone" requirement, but consideration of that problem leads one to question why recording devices attached to telephones should be treated differently from other participant monitoring of telephone conversations and why participant monitoring of telephone conversations should be treated differently from participant monitoring of face to face conversations. Often social issues must be attacked in pieces because the agencies willing to act have authority only over particular aspects of the issues, but it is useful to understand what lines a more comprehensive approach would take.

In respect to participant monitoring there are at least three important variables: who is monitoring; for what purpose; and by what means. Law enforcement monitoring is quite different from private monitoring designed to embarrass someone who speaks freely about his personal life.

Some methods of monitoring destroy ordinary expectations more than others. In face-to-face conversations each party is able to see those evidently within hearing range, and any use of electronic devices to record or transmit the conversation to others is inconsistent with the expectations of the party who has not consented. Matters are more complicated when the telephone is used. Callers know that family members and secretaries sometimes listen at extension telephones, or are allowed to hear what is said by recipients who merely hold the telephone away from their ears. It undoubtedly evidences more respect for the caller's privacy if he is explicitly made aware that someone else is listening; but the caller sometimes supposes without being told that an extension phone may be in use, especially if the receiver clicks when it is raised or the caller hears breathing or background noise from the extension. Many offices have speaker phones which put the telephone sound system on a speaker, and allow a telephone call to be broadcast to an entire room, in which many persons may be seated. Apparently, even if not told the caller can ascertain when such a system is being used because the quality of the recipient's voice is altered by the fact that the microphone into which he speaks is typically a few feet away from his mouth rather than the few inches that separate a speaker from the mouthpiece of an ordinary telephone. Another device that may be used for monitoring is a transmitter cut-off switch, which permits a person to listen at an extension without any noise being transmitted from the extension. Though some persons are aware of the risk that cut-off switches may be used, others would be surprised and many would be disconcerted if cut-off switches were used to facilitate monitoring without their consent.

In most situations actual recording of conversations cuts more deeply into the caller's expectations than the recipient's allowing others to hear, and this is so whether or not the recording device is electronically attached to the telephone, physically attached to the telephone or simply set near the receiver.

Recording devices or other forms of participant monitoring may be used for a number of purposes. I have already discussed the obvious advantages to law enforcement work of having an accurate record of a conversation. Monitoring can also help a participant in a conversation who fears that another participant may later give a false account of it. For example, an official offered a bribe may be as interested to establish his own innocence of wrongdoing as the guilt of the person who has offered the bribe. The interest in scientific observation of spontaneous interaction sometimes underlies electronic monitoring, as it does the use of two-way mirrors. For example, my two-year-old child attends a playgroup twice a week at Barnard College; students in psychology courses observe the children at play through a two-way mirror and what the children say is electronically transmitted to the observation room. Monitoring may also be useful for purposes of treatment. A psychiatrist, for example, might record a patient's remarks to have a precise recollection of them, but fear that if he told the patient about the recording the patient's remarks would be less spontaneous.

In considering how participant monitoring should be regulated, let us first consider government monitoring. In 1967 Ramsey Clark, then Attorney General, issued a memorandum to heads of executive departments and agencies in order to curtail consensual monitoring as well as third party wiretapping and eavesdropping. With respect to telephone conversations, agencies were instructed to adopt rules governing interceptions "under circumstances where a party to the conversation has consented. Such rules shall, where appropriate, provide for the advance approval by the agency head of such interception." With respect to nontelephonic communications in which not all participants had consented to recording or overhearing, agencies were directed to "obtain advance written approval from the Attorney General for any use of mechanical or electronic" monitoring devices. See Appendix H to FCC Monitoring of Employees' Telephones, Report of Special Subcommittee on Investigations of House Committee on Interstate and Foreign Commerce, H. Rep. 92-1632, 92d Cong., 2d Sess., 1973, pp. 63-65.

The 1967 instructions are still in force and the various agencies have their own policies on telephone monitoring. For a summary, see Telephone Monitoring Practices by Federal Agencies, Hearings Before a Subcommittee of the House Committee on Government Operations, 93d Cong., 2d Sess., 1974, pp. 202-203. It is evident that as a consequence of the furor over "Watergate" and the prodding of Congressional committees, agencies in the past two years have become much more careful in developing their own guidelines and inducing their observance, but it is still impossible to estimate how often agency rules about telephone monitoring are broken and how often monitoring of nontelephone conversations is done without the required permission of the Attorney General. Widespread publicity within the Executive Branch about present restrictions, as well as effective sanctions, are called for; but a systematic assessment of when monitoring is acceptable is also needed. Some agencies forbid all monitoring without the consent of all parties; others allow monitoring of telephone calls when only the government official has consented. And the variation in policy often does not reflect any obvious difference in agency function. While important differences in functions may appropriately lead to different policies, there should be some consistent approach to monitoring within the Executive Branch.

Monitoring is an appropriate method of collecting evidence of crime, but the mere possibility of such evidence is not sufficient to allow agencies to monitor their contacts with citizens on a

routine basis, whether these contacts take place in offices or over telephones.

Four Justices of the Supreme Court believed in *United States v. White*, 401 U.S. 475 (1971), that monitoring without probable cause and a court order was unconstitutional. It would be a good idea for Congress to impose such requirements for law enforcement monitoring, perhaps by amendment of existing legislation on wiretapping and eavesdropping. If the court order standards of that legislation are thought to be too strict, then at the least the law should contain some system of prior review when feasible and some requirement that monitoring only be employed when there is a substantial probability of obtaining relevant evidence. It might be argued that monitoring by open government agents, such as an Internal Revenue officer making an income tax audit, should be permitted more freely than monitoring by undercover agents, on the theory that one who speaks to an obvious government officer should not object if what he says is transmitted reliably to other government officers. But, since persons are often more open and less circumspect in conversation with one person than when they are speaking "for the record," monitoring even by an acknowledged officer does intrude on privacy, and its widespread employment would inhibit many useful interchanges between citizens and government officials. Therefore, routine monitoring should be forbidden even to open officers whose work has law enforcement implications.

Similar principles should apply when a government official monitors to "protect himself" against the other party's recounting an inaccurate version of a conversation. Indeed frequently the occasions for "protection" will also be those when incriminating admissions are likely. Whether monitoring should be allowed in any situation where it has been made clear to the citizen that he is a suspect whose admissions will be used against him is a more difficult question which I put aside here.

Assuming circumstances in which recording or monitoring by special electronic devices should be restricted, should government officers at least be able freely to have secretaries listen surreptitiously on extension telephones? I believe the answer should be "no"; in ordinary circumstances the government should set a model for straightforward dealings and, in the absence of strong justifications in particular instances, it should not engage in deception about the conditions of its conversations with citizens. Although transmitter cut-off switches were originally designed for places of intensive background noise, such as machine rooms, their main use by government agencies is in ordinary offices. The gain in cutting off the background noise in such offices is not great enough to offset the increased risk of surreptitious monitoring, and government agencies should get rid of these devices unless surreptitious monitoring is deemed to be often appropriate for the telephone in question, or background noise is either very loud or should not be transmitted for some special reason (e.g., it consists of conversations about sensitive secret matters).

I have not discussed conversations between government officers themselves, conversations which "Watergate" disclosures have revealed were subject to considerable monitoring during the Nixon Administration. Although it might be argued that officials have less legitimate expectations of privacy than ordinary citizens, I should assume that their privacy in ordinary working relationships does deserve protection and that basically the same principles should be applicable to their conversations with each other as to conversations between citizens and officials.

Probably the most typical form of monitoring within government agencies as well as private companies is not designed to ensure a record of what callers say, but is for what the telephone companies call "service observation" or "supervisory observation." Service observation involves monitoring to see that equipment is working properly; "supervisory observation" involves monitoring to be sure that employees are performing effectively and to determine how they can be more adequately trained. For

example, the Internal Revenue Service gives taxpayers information over the telephone. The most effective way for supervisors to know if accurate information is given in a polite way is to listen occasionally to calls in which information is given. Does this intrude on the privacy of the caller? Some government officials have argued that it does not. See Telephone Monitoring Practices by Federal Agencies, *supra*, at p. 284. The argument is essentially this. Most callers do not give their names. They are not calling a particular government official but anyone who can give them information. Since they are willing to say whatever they have to say to an official they do not know, they have no interest in being heard by only one official rather than two, no interest in being heard only by a subordinate rather than supervisory personnel.

This argument is powerful when applied to the routine calls for information that some private companies and government agencies may receive, but it is overly simplistic in relation to calls for tax information. Callers typically relate personal facts and ask about their impact on tax liability. Frequently they do leave their names in order to be called back with further information or to be sent appropriate forms. Sometimes the official giving information or sending forms may elicit acknowledgments of tax liability. For example, an acquaintance of mine, having hired fulltime domestic help, recently telephoned and asked for the forms he would use to pay applicable social security taxes. The official's first question was whether he had ever paid any domestic help, including once-a-week help, more than \$50 a quarter before. It is safe to assume that a high proportion of Americans who have domestic help once a week or every other week do not pay social security taxes and probably do not even know they should; so for many people a full answer to the official's question would involve an admission of unpaid tax liability. Whether or not this official would transmit the admission to other officials responsible for tax collection, the caller might understandably fear that possibility; and he might well be uncomfortable if he thought two officials including a supervisor had listened to his responses. Even if a caller does not leave his name, he may have an irrational fear that his call has been traced or that he has divulged so many facts his return could be identified. As unrealistic as such fears may be, it is only with some hesitancy that many taxpayers divulge relevant facts to officials giving information; and many do rely to some degree on the assumption that they are not being "ganged up on" at the other end of the telephone. Widespread knowledge that calls for tax information are monitored would almost certainly have some effect on taxpayers; in some instances it might discourage avoidance of liabilities; in many more it would discourage taxpayers from getting information from the government rather than private tax advisers. Of course, the effect would be muted if the purpose of monitoring were fully explained, but many persons would continue to worry about communications between information officers and enforcement officers.

In response to Congressional concerns, the Internal Revenue Service has agreed that "tax packages (will) include a notation that the service monitor, for quality purposes, a random sample of tax information telephone calls." See Letter from Commissioner Donald C. Alexander of July 3, 1974, in Telephone Monitoring Practices by Federal Agencies, *supra* at p. 286. This is a useful step, although it remains to be seen whether this procedure will make most taxpayers aware of the possibility of monitoring. More satisfactory notice would be given by requiring such a statement at the beginning of each relevant telephone conversation, or by requiring a "beep-tone," or by following Georgia and requiring an asterisk by the telephone listings of agencies that monitor calls.

The main point I wish to make about monitoring for "supervisory observation" is that it is difficult to generalize about its impact on privacy. For some really routine calls, it may not be inconsistent with any important expectations of the caller;

but for other calls, and I would count many tax information calls among these, it does intrude on significant expectations of privacy.

How monitoring by private persons and companies should be treated is in some respects even more difficult to decide than what should be done about government monitoring. Consider the following example related to me by a colleague. A woman is shot at by an intruder in her home. That evening she says she can not identify him, but subsequently she says the intruder was her ex-husband. He is then prosecuted for attempted murder. The lawyer for the ex-husband, because of the delay in identification, the ex-wife's extensive psychiatric history and his client's convincing alibi, is quite sure he is innocent. The ex-wife and the ex-husband continue to converse over the telephone about support payments and visitation rights. The lawyer, fearing that the ex-wife may testify falsely about a telephone conversation, advises his client to record their conversations. Shortly before the trial the ex-wife says over the telephone that she will withdraw her complaint if the ex-husband increases support payments. The lawyer uses the recording at the trial when the ex-wife denies having made those remarks. The original purpose of the recordings was essentially "protective," both in the sense of protecting the husband against assertions that he said things he did not say, and in the sense of preventing conviction on unwarranted charges. The ultimate use of the recording at trial was protective only in the latter sense; it was "aggressive" in the sense of establishing that the ex-wife had said damaging things she then denied. It is difficult to say, especially in retrospect, that such recording was not justified, but it is presumably covered by the "beep-tone" rule. The Federal Communications Commission has recently said that the rule does not apply when the recipient has good reason to believe the caller's remarks will involve commission of a crime (e.g., blackmail) or violation of company tariffs (e.g., abusive telephone calls). See *Maller v. New England Telephone Co.*, 44 F.C.C.2d 614 (1974). It is doubtful if the ex-wife's remarks in the final conversation would qualify on one of these bases; certainly the original recordings could not be justified under either exception.

Private monitoring, whether of face-to-face or telephone conversations, should not be made criminal if it is based on a reasonable effort to establish wrongdoing, to protect oneself, to engage in treatment, or to make scientific observation possible. Monitoring for service or supervisory observation should also not be made criminal, but when a company does engage in such observation, there seems no good reason not to notify those telephoning the company of that fact. Other uses of monitoring whose propriety is at least arguable may also be established; but monitoring for less positive purposes should generally be banned. The present statute on wiretapping and eavesdropping aims at some such distinction, 18 U.S.C. Section 2511(2) (c) and (d), but its language can be reformulated to increase coverage.

As far as private persons are concerned, probably monitoring that involves only use of ordinary telephone equipment and no other device should be allowed generally, since it would be harsh to make simple listening on extension telephones a crime. It would make sense to continue and strengthen restrictions on the use of recording devices, however, since these restrictions can supplement applicable criminal sanctions. Appropriate exceptions should be recognized; but coverage should be broadened to reach any combination of telephone and recording device, not only the electrical connections reached by the present "beep-tone" rule. It might also be wise to limit the use of devices like transmitter cut-off switches to telephones as to which a substantial need for them can be demonstrated. When such devices are used to permit a third person to hear a conversation, notice should be provided.

CHAIRMAN ERICKSON: Professor Uviller.
[Whereupon, Mr. Uviller was sworn by Chairman Erickson.]

TESTIMONY OF H. RICHARD UVILLER, COLUMBIA UNIVERSITY SCHOOL OF LAW

CHAIRMAN ERICKSON: Professor Uviller is also of Columbia School of Law, formerly Chief of the Appeals Bureau for the District Attorney in New York City, Frank Hogan. While there he argued the *Berger* case for the State of New York in the United States Supreme Court. Professor Uviller believes, as I understand it, that the wiretapping statutes need considerable revision.

And if you have an opening statement to make, we will listen with great interest.

MR. UVILLER: Thank you, Mr. Chairman.

I am pleased to be here and participate in your important work. I am also sensitive to the limits of patience and courtesy in proceedings of this nature. The hour is late, and I do appreciate the opportunity to be able to say a few words before you adjourn.

I have come in some haste and I was unable to submit to you in advance a written statement, but I have brought with me, and I believe you have now before you, a rather brief and somewhat informal, perhaps ill-documented summary of some of my comments and reactions to the law as it stands and to the principles which have concerned you today and throughout these hearings.

I intended to paraphrase or summarize that written document orally, but as I have been listening here today it has occurred to me that perhaps it would be better for me to address some of the issues which have arisen during the colloquy that preceded my testimony and leave the document to speak for itself, inadequately as it may, on other matters.

In introducing myself, I would have included among my rather sparse qualifications for this role the fact that I was the principal draftsman of an eavesdropping law for the State of New York which passed shortly before Title III became law and superseded it. It had perhaps the shortest life of any piece of legislation of this importance insofar as it became obsolete almost immediately upon its enactment.

I feel that Title III in many respects conformed with my view of the matter at that time, although in many particulars the legislation for New York differed from Title III.

I will try to forget the pride of authorship which I felt at that time. However, there are a number of

items in which I think I will inevitably revert to choices made in that piece of legislation, which I still think are preferable to choices that are reflected in Title III.

Let me open by commenting on some of the issues which have been raised during colloquy in reverse order.

As I listened to my colleague, Kent Greenawalt, I almost wished that I could be in his place and address those very same questions from my own perspective, not because I differ from him materially, but because I do think that they reach the heart of many of the crucial issues which confront you, and I would like very much to share with you my views.

Indeed, I think that Professor Greenawalt and I share the same general approach and perspective on electronic surveillance, and as a preliminary matter perhaps I should try to identify my own position with respect to this device of law enforcement.

I am among those who believe that electronic surveillance is a crucial tool for the investigation of a number of extremely important crimes and other social problems.

I would be extremely hesitant, despite the emotional appeal of much that General Clark has said—I would be extremely hesitant at this juncture to deprive law enforcement agencies of this device, and the very substantial benefits which I believe can be derived from its proper employment under proper supervision.

So, consequently, I would have to agree with the Chairman and say that I am one who approves of electronic surveillance. I do not see any necessary antipathy between electronic surveillance and other forms of search and seizure or between the Fourth Amendment and eavesdropping.

I do believe, however, that electronic searches are peculiarly and particularly intrusive on some very important values of our society: fearless verbal intercourse. But I think that great as these intrusions are, they are greater only in degree from the intrusions suffered by citizens through conventional search and seizure, and not different in kind. I think that they are, with some difficulty, admittedly, susceptible to the same sort of control and supervision which the Fourth Amendment applies to conventional searches and seizures.

To comment, then, on some of the issues which have been raised in previous colloquy, let me take up, first, if I may, since it is freshest in my mind, the notion of an expectation of privacy as the heart principle, the crucial principle, in these matters.

In this I suspect that Professor Amsterdam is correct when he states that the casual encapsulation of the *Katz* decision into the legend "expectation of privacy" is facile, if not erroneous. I don't think

that the Supreme Court intended or could have intended to describe the Fourth Amendment as protecting only those aspects of one's personal life in which one has an expectation of privacy.

If that were the case, then a citizen leaving an automobile parked on the streets of New York where there is substantial risk that it will be broken into would have no Fourth Amendment right against the police doing what a burglar is likely to do.

If one lives in an area in which burglary is common, one has no real expectation that the contents of one's home are immune from strangers' probing fingers; but even without that expectation, one certainly could not argue that a search warrant was not necessary in those areas.

CHAIRMAN ERICKSON: May I just ask at this point: Are you saying that the Fourth Amendment would offer some protection against burglary? I thought this was related to law enforcement personnel.

MR. UVILLER: I say the *Katz* interpretation of the Fourth Amendment cannot be taken to reflect the actual, real expectation of privacy or freedom from intrusion, because in many areas in many of our cities there is no real expectation of freedom from intrusion. There is no real expectation that the locks on one's front door or on one's car door will keep the world out.

Consequently, we cannot take the Fourth Amendment as reflecting that unfortunate state of affairs, but rather, as I think Stewart intended it, the reasonable expectation of privacy, by which we mean the expectation which one is entitled to have—not the expectation of privacy that one actually has.

In that respect, it may be that Mr. Justice Harlan had a point when he said that one cannot divorce the reasonable expectation of privacy from the place in which the private conversation is held or the place in which the personal effects are stored.

Speaking of the prison as a problem area, the reasonable expectation of privacy frequently follows the law. That is to say, insofar as the courts have held that no warrant is necessary to intercept conversations between prisoners in prison, then prisoners have no reasonable expectation of privacy in those conversations. However, should the courts hold to the contrary, then the reasonable expectation of privacy would follow the law.

In fact, when we say the Fourth Amendment protects a reasonable or legitimate expectation of privacy, all we are really saying, I suppose, is that the Fourth Amendment protects privacy insofar as the law and the courts have accorded protection to privacy in that particular place, or in communications of that nature.

So that the "expectation of privacy" tag or rubric for description of the scope of Fourth Amendment protection fails for circularity. The law protects what the law protects, and the law does not protect what the law does not protect.

I find that a profitless course to follow in an attempt to determine such difficult issues as whether or not a search warrant is necessary to tail a man, perhaps tail a suspect by electronic devices; whether the Fourth Amendment protects one against telephoto lenses or, indeed, whether the Fourth Amendment protects one against a faithless companion who is actually an undercover agent or police informant.

It seems to me the only way in which we can attempt to describe the protection of the Fourth Amendment is from first principles, that is to say, where and in what respect does a citizen have the right to reject intrusive curiosity of the state?

I believe that there are a number of "public" and "private" distinctions that might be made, that is to say, what one does in public with its knowledge and expectation that the world at large would perceive him is hardly the sort of activity which one can claim is immune from police or official observation.

That, perhaps, describes that area of the problem which Professor Blakey asked Professor Greenawalt about, having to do with public meetings, public activity, and the like—that is to say, public in the sense they take place in full view of an undifferentiated public.

This line of reasoning might, however, lead to a startling conclusion with respect to activities that take place in private, but with another individual. The so-called consensual eavesdropping which has concerned members of the Commission today is a communication with another person where the person being surveilled neither knows nor has reason to know that the person to whom he is communicating is, in fact, a police officer in disguise.

It may well be that that situation, the Hoffa situation, is as much of an intrusion on legitimate expectation of privacy as the use of electronic devices to reproduce the conversation more accurately.

I see no distinction (I'm agreeing with the dissenters, in fact, in the *White* case) between electronic surveillance or electronic recording, and the use of spies and informers. I am led to the conclusion that perhaps court supervision is required to use the recollection of a purposely implanted spy as well as the recording that is made with that person's knowledge and consent.

And I do not regard one of two conversants secretly taping a conversation as analogous to a third-party eavesdropping, but I do see it as very close to an unrecorded conversation which is being reported to police by a human agent.

I think there has also been some discussion here about the matter—

CHAIRMAN ERICKSON: Without trying to interrupt—

MR. UVILLER: I wish you would, Mr. Chairman.

CHAIRMAN ERICKSON: I would like you to give me the rationale for saying if I come to you, a friend of yours, and you tell me about a crime that has just been committed, and I have been sent there to talk to you by the police, why it would be that there should be a court order before I could talk to you to elicit this information, even though I go there on behalf of the police?

MR. UVILLER: Well, as I say, I see no difference whether you are wired or unwired. Consequently, I have reached the same result, whether it was a question of your oral report or your recorded report—the same result.

I do say that it is conceivable to me that in discussing the matter with another human being, any citizen is entitled to believe that that person is what he appears to be, that is to say, a private individual. It is true he takes certain risks. He takes the risk that the person may turn against him in the future and prove to be faithless and go to the police and incriminate him. That is, I think a normal risk.

But I do not think that we, as citizens, must take the risk that the person who appears to be an ordinary private person is, in fact, a covert police officer, and consequently—

CHAIRMAN ERICKSON: Or was sent there by the police.

MR. UVILLER: A police officer or agent of a police officer. In other words, I am simply turning around the human microphone analogy and saying that when the police officers send a spy into a person's private life in order to perceive and report what he says, they are, in fact, installing a bug, a somewhat inaccurate bug, perhaps, but in effect a bug. And there is no reason to believe, as the court said in *Hoffa*, that that person is not only potentially faithless, but actually functioning as a police informant.

I believe that in the *Hoffa* case the error was that the court said that it's part of one's daily life, that it is part of normal human intercourse, to assume the risk that another human in whom one confides will at some point under some circumstances confide that incriminating information to the authorities.

CHAIRMAN ERICKSON: I think that was in *Osborn*, not *Hoffa*; am I right?

MR. UVILLER: I could be wrong. I thought it was *Hoffa*. But in any event, that may well be true. Perhaps that is part of the normal risk, but I am not sure that it is part of the normal risk that we are all

forced to take in effect that the person was purposefully sent by the police into one's company for this specific purpose.

CHAIRMAN ERICKSON: Are you going so far as to say that there is a right of privacy between the conspirators?

MR. UVILLER: There is no right of privacy between conspirators who are at the time of the conspiracy and communication acting as private persons. But if one of those purported conspirators is a spy, an infiltrating police agent, I say that there may very well be.

In other words, the court in *Hoffa*—it made no difference, they said, whether Partin was purposely sent to spy on the defense camp or whether he spied for his own purposes and reported later spontaneously. They said that was not the crucial issue.

And where I say they may have taken a false step is that may be a crucial issue. And where the police know enough in advance to obtain an inside ear or to send a police officer as a false confidant, that they have enough to get permission of a court to do so; and that sending a police agent secretly into the company of another may be sufficiently analogous to the planting of an electronic device, and surreptitiously and secretly, such that the analogy would require a court order.

I am not suggesting, however, that is strictly within your mandate as far as we are speaking here of a report unaided by conventional electronic means, neither transmitted nor recorded, but simply reported by a spy.

I do say I think there is a closer analogy between an electronic bug and a spy than there is between a body recorder and a bug.

CHAIRMAN ERICKSON: Are you putting this more or less on the vein of an extension of entrapment, for example?

MR. UVILLER: No, I think entrapment is entirely different.

CHAIRMAN ERICKSON: I would think so.

MR. UVILLER: Factually it may not be entirely different. It may be that the spy acts as an entrapper, an agent provocateur, and the line is difficult to draw.

But, at this point I am only speaking of the agent who passively participates in the conspiracy, specifically for the purpose of reporting conversations to the authorities, acting, if you will, as a transmittal or memory device without electronic assistance.

There has been also some colloquy here with respect to the limitation of electronic surveillance according to the crime being investigated.

MR. BLAKEY: Professor, could I interrupt on that just to maintain the continuity of what we are talking about?

MR. UVILLER: Certainly.

MR. BLAKEY: When you suggest that an informant is a walking bug or a bug that walks, I take it what you are saying is not that we shouldn't use informants, but that we should subject them to judicial supervision?

MR. UVILLER: Professor Blakey, I am a great believer in procedure, and it is not altogether naivete on my part, nor is it simply the formalistic virtues of complying with the language of the Fourth Amendment itself.

I believe that there is great benefit in requiring resort to the courts, not so much because the individual judge to whom the application is made will, in the large majority of cases, function as that neutral and detached magistrate which we all say he is, but rather because I believe it exercises a healthy restraint on administrative and law enforcement agencies to force them to put their suspicions in writing and to submit them in advance to some third party.

Wholly apart from the internal scrutiny that may be exercised over affidavits within a good law enforcement office, I simply think that reducing something to writing, putting it in a formal application which becomes a part of the official court record—

MR. BLAKEY: We don't need a judge for that, do we? We could have a recorder of affidavits who could file it and date-stamp it.

MR. UVILLER: We could, and very largely that is the function that courts have performed. But often the prosecutor or police believe the judge is going to exercise some intelligent review, and perhaps they sometimes do. So I do like the system of submitting applications to judges and making the applications as formal as possible before the fact, and subject to review after the fact. So I suggest the warrant procedure be extended rather than eliminating searches and seizures.

MR. BLAKEY: You know the origins of the search warrant process. It is a very old institution—the memory of man runneth not to the contrary when it first appeared in common law history. It seems to have been sort of a writ of replevin to recover the stolen property. That was the kind of intellectual model around which the search warrant developed.

That is not what we are talking about any more. We are performing entirely different things today by a warrant process in the 20th century than we did in the 16th.

I would wonder how you would take things like probable cause and adapt them to what is a very different use of the warrant process. I refer now particularly to the consensuals, which have been a continuing problem for this Commission.

For example, one typical use that is made of consensuals is in narcotics cases. A Kel device is placed on an officer in order that other officers may monitor the transaction, not really to recover stolen property or some specific item, but rather to protect the life of the officer.

And I am told by officers in the field that it would be difficult in all cases to show specifically case by case that there was a reasonable expectation of danger, i.e., probable cause to believe that this officer on this occasion in this transaction might be subjected to violence.

If I apply a traditional probable cause type standard saying that you can only use a Kel device where you have probable cause to believe that danger will occur, it seems to me in a significant number of cases you could not get a warrant to use the Kel device, and what we'd then be doing is asking the officer to run an unnecessary, in my judgment, risk of physical danger. That certainly would have to be put in the balance against the privacy expectations of the party being overheard.

I wonder if you'd comment on that problem, and particularly the notion that should we apply probable cause here like it has been applied in the past.

MR. UVILLER: Yes. It is a very difficult matter. We certainly have, as you have indicated, rid ourselves of any lingering notions that the Fourth Amendment is applicable only to objects—the use of the words “things” in the Fourth Amendment notwithstanding. We now believe that words—even words that have not yet been uttered—are subject to search and to seizure by electronic transcription or otherwise.

So, too, I think the probable cause standard, insofar as it had a “strict construction” in the early times, has become a much more flexible notion.

I used to think that probable cause meant at least a prediction was more likely to be true than not. I learned in the *Peters* case from the Supreme Court that that is not necessarily true.

I used to think that there had to be a particular reason to believe that a particular intrusion would be productive before a warrant could issue. I learned from the Supreme Court in *Camara* that that is not necessarily true.

The Fourth Amendment, it seems, can be satisfied and probable cause established merely by showing that a particular procedure is reasonable, that it is appropriate in the circumstances, that it is not any more intrusive than is required by some regular social need or process. And I think that the notion is today sufficiently adaptable, that it is almost true that the first clause of the Fourth Amendment dealing with unreasonable searches and seizures has become amalgamated with the term

"probable cause" in the warrant clause, the second clause of the Fourth Amendment.

There has been a lot of debate, as you well know, about the distinction between those two clauses and the relationship between the word "reasonable" in one and the term "probable cause" in the other.

I am led to believe by recent decisions of the sort I mentioned that there is almost no distinction between those two concepts today, and therefore that probable cause could be found merely upon a showing that the procedure was necessary for a legitimate social purpose.

By the way, that would be another criticism of the act which I think I mentioned in the statement, although I didn't plan to allude to it orally. And that is this: The act seems to be focused on the acquisition of evidence of crime.

MR. BLAKEY: Could we stick with this?

CHAIRMAN ERICKSON: I would like to do this: Professor Blakey and I will be here until this hearing is over, but we have got a couple of people that won't be, so if we could get you to finish your prepared statement—

MR. REMINGTON: Mr. Chairman, don't think Chief Andersen and I have serious time problems. I don't have to leave until 7:00 o'clock.

CHAIRMAN ERICKSON: Fine.

For the purposes of the record, the Draft of Testimony to the National Commission on Eavesdropping bears the date of June 10, 1975, and may we file this as part of your testimony.

MR. UVILLER: I apologize for the informal caption on that, Mr. Chairman. It merely represents the haste in which it was prepared.

[The document referred to follows.]

STATEMENT OF H. RICHARD UVILLER COLUMBIA UNIVERSITY SCHOOL OF LAW

Introduction

I am pleased to have been invited to participate in the important matters covered by your mandate. Surely, one of the best features of the design Congress adopted for the regulation of electronic eavesdropping was the provision for periodic review and revision. You have already heard from many witnesses more scholarly, pragmatic, and devoted to the field of surveillance and privacy than I. I am not at all confident that I will be able to contribute either analysis or experience as valuable as theirs. Yet, I can not resist the opportunity to offer some reactions and observations of my own on this vital and controversial topic.

Let me briefly introduce myself. I am a member of the faculty at Columbia Law School. My field of principal pedagogical and scholarly interest is the criminal process. Prior to joining the law faculty in 1968, I was for 14 years a member of the staff of the late great Frank Hogan, District Attorney in the County of New York. As chief of his Appeals Bureau, I had a hand in the formulation of office policy, as well as the review and argument of numerous cases. I had some exposure to the uses of eavesdropping in my contacts with the investigative bureaus of the office, and

brought my full attention to the problem in the briefing and argument to the Supreme Court of the case of *Berger v. New York*. Thereafter, I took a hand in the drafting of a statute for New York governing electronic surveillance. Although that statute became law in New York, it had a remarkably short life, for within a matter of days of its effective date, it was superseded by Title III of the Omnibus Crime Control and Safe Streets Act. While there were many similarities, there were several differences between the two pieces of legislation. I shall try not to let any lingering pride of authorship in the first enactment color my criticism of the Act which displaced it.

Further, by way of introduction, I think I should attempt to state my general position with regard to electronic surveillance. I am among those who believe that, in a significant number of instances, acquiring evidence by electronic means is essential to the successful prosecution of important crimes. Further, I believe that a court order authorizing such an acquisition may be convincingly analogized to a warrant for a conventional search and seizure; in my opinion, there exists no necessary antipathy between the Fourth Amendment and eavesdropping. At the same time, I recognize (as we all do) that this form of government activity is particularly threatening to personal privacy and the secure enjoyment of that inestimable value of a free society: fearless verbal intercourse. I know, too, that authorized eavesdropping is particularly prone to abuse. I have witnessed the operation of the Law of Official Insatiability, the bottomless appetite of law enforcement agencies (and other government organs) for "intelligence" concerning the daily activities and affairs of large numbers of private citizens, groups, and business enterprises. Moreover, I acknowledge that electronic searches strain some precepts and traditions of Fourth Amendment law.

Accordingly, I favor a specially and severely circumscribed statutory structure for the employment of electronic surveillance. In other words, the authorization is only as good as the limitations which accompany it.

GENERAL PRINCIPLES

I shall presently address several comments and criticisms to the specific provisions of the law under consideration. But first, let me attempt to enumerate what I deem the irreducible requisites of a wise and constitutional statute governing electronic surveillance:

1. It should clearly and unambiguously withhold authority for all ventures seeking general or "strategic" intelligence concerning a suspect activity or target. To this principle, I would append only one possible exception covering investigations of peril to the "national security." And it must be obvious to all Americans in the present era that the term "national security" itself requires scrupulous and careful limitation by precise definition.

2. Eavesdropping should be permitted only where there is a reliable basis for the belief that it will produce evidence essential for the prosecution of a particular crime, the apprehension of a particular individual, and the remedy or prevention of substantial harm. Law enforcement agencies should not have access to this extraordinary technique to acquire mere supplementary or cumulative evidence which might strengthen a case fit for prosecution without it.

3. The statute must assure that in every instance of its employment, surreptitious eavesdropping is actually and in fact a device of last resort. Mechanical recitation of a conclusory formula regarding alternative investigatory methods should not suffice to actuate the extraordinary techniques of electronic surveillance. Only where it is demonstrated and determined that comparable evidence is unavailable and can not be obtained by other means should resort to electronic surveillance be authorized.

4. Despite the multifarious activities of target criminals and the multitiered structure of the "underworld," the law should reserve the peculiarly intrusive penetration of electronic sensors for cases of unusual gravity or situations of unusual and im-

mediate danger. Moreover, Congress should not delegate to the state the composition of an unlimited list of crimes the investigation of which warrants the use of electronic eavesdropping. The list is likely to be too inclusive, and the electronically aided investigations too likely to probe common and trivial instances of the designated crimes.

5. Because one of the more onerous aspects of the "generality" of eavesdropping inheres in the duration of the surveillance, and because "minimization" is difficult to achieve in other ways, the period of an initial reception should be as brief as possible. In most cases, the order should be self-terminating upon the acquisition of the evidence sought. And the outer time limit on the effort to obtain evidence should be short. More importantly, extensions of the original order should not be readily granted, and in no case merely upon a renewal of the original application and a reiteration of the original bases for probable cause. Only upon a showing of new facts, from the original monitor or otherwise, should continued surveillance be authorized. A fruitless surveillance should never provide the reason for its continuation.

6. Applications for eavesdropping orders should be made only by the superior prosecuting officer of the jurisdiction personally, or by a designated deputy acting in his stead in the absence of the senior official; never should a police or investigative agency official take the responsibility for initiating an electronic surveillance by application in his own name.

7. All identifiable persons whose words have been intercepted by the eavesdrop should receive subsequent notice of the "seizure" regardless of whether they were named in the authorizing papers or eventually become defendants. Only for specially demonstrated cause should the court direct that such notice (or "inventory") be withheld.

8. The code embracing all regulations should be as simple and generally comprehensible as possible; it should be framed unambiguously, with careful precision, and in readily readable form.

In the foregoing enumeration of basic tenets, I have consciously omitted a number of issues. These omissions do not reflect my lack of concern, but rather the difficulty of articulating positions with regard to them. In addition to the matter of the definition and exemption of "national security" investigations, these other matters include:

1. coverage of extension telephones and party lines;
2. extension to "pen-registers," commercial information relayed to or from computers, and like transmitted data other than personal "communications";
3. extension of the concept of "search and seizure" to the surreptitious recording or transmission by a consenting wired participant in an otherwise "private" conversation.

SPECIFIC CRITICISM

Let me now turn to a consideration of a few selected features of the current law wherein I believe reconsideration and revision may be advisable. I have tried in the paragraphs that follow to be brief and exhibit a due regard for the natural limits of patience and courtesy. I have therefore eschewed mention of matters of form and style only, although I consider these to be matters of some importance. Too, I have not fully supported my comments by argumentation or the citation of authority. And finally, I can not warrant that the following constitutes an exhaustive list of my discontents.

By way of preface to my critical comments, let me say that I find much in the Act sound and commendable. At the very outset, we should not overlook the excellent achievement of its enactment. We tend to forget how long and hard it was to secure a comprehensive regulation penalizing unlawful eavesdropping and allowing strictly circumscribed surveillances under court supervision. The old section 605 of the Communications Law was hardly an adequate piece of federal legislation for our electronic age. Thus, whatever its infirmities, whatever the scars of political

compromise it may bear, we should be duly thankful to have Title III to work with and to improve upon.

Nor is the Act a cheap or facile law. It is thorough and detailed. It is strong and comprehensive. At least on its face, the law has the teeth of enforceability in its condemnation of unlawful electronic interceptions.

"Last resort"

I find the purpose of the Act plain and praiseworthy insofar as it regards authorized eavesdropping as a "last resort" measure. Sections 2518 (1)(c) and (3)(c) both express this feature, reserving the employment of the Act for those cases in which other "normal" means have been fruitlessly attempted or are obviously doomed or dangerous. I may be quibbling when I note in passing that the term "too dangerous" is somewhat uncertain as it stands. Danger is a normal ingredient of criminal investigation. Indeed, a surreptitious entry to execute an order for the installation of a sensor might be regarded as a highly dangerous sortie. I would therefore attempt to define "danger" at least in terms of the type of harm and the person imperiled to add credence to the choice of the electronic alternative.

"Plain view"

I also approve what I term the "plain view" acquisition section (§2517[5]). I believe it fairly comports with evolved constitutional doctrine on the subject. I regard the provision as wise and necessary from a policy perspective. And the additional safeguard of post-facto validation of the windfall acquisition affords an appropriate means of assuring a bona fide and good faith procedure rather than the sham and pretense which occasionally cause concern in the ordinary "plain view" situation.

"Minimization"

Further, the Act's reference in Section 2518(5) to what has come to be called "minimization" was a wise, if somewhat casual, provision. I favor its retention. However, I do believe that, particularly in view of the attention this provision has received in recent litigation, it should be clarified in two respects: first, the nature of required care against overbroad reception and recording should be specified; and second, the consequences of failure to take appropriate precaution should be determined. In other words, was it, and is it the intent of Congress that an agent's failure to cease recording an irrelevant conversation precludes the subsequent use in evidence of an incriminating conversation recorded on a different day during the term of the interception? I gather that two lines of judicial thought are developing on the severability of indiscriminating execution. It is not an easy conflict to resolve, particularly in the light of the inherent uncertainty of proper procedures of minimization. But it requires careful legislative attention and expression.

"Strategic intelligence"

Moving now to a number of specific provisions of the Act which occasion somewhat stronger doubts and misgivings, I should like to tackle first the important matter of the "strategic" or "intelligence" eavesdrop. On first encounter with Title III, I thought that Congress had rebuffed the data-collectors, reserving authorization for the evidence-seekers alone. On more careful reading and further reflection however, I am no longer confident that the Act by its terms does not tolerate the employment of electronic surveillance where there is probable cause to believe that a particular individual will engage in a conversation revealing participation in, or the purpose to participate in a future crime of a designated sort. "Keeping tabs" on a suspect in this manner, listening and waiting for the evidence of a future crime, I regard as "strategic surveillance." If it is permitted under the Act, it should not be; if it is practiced under the Act (as it may be), the Act has failed in an important way. For, in my opinion, such open-ended searches are basically antithetical to the Fourth Amendment.

True, Section 2518, paras. (1)(b)i, (3)(a), and (3)(b) all insist that the order relate to a particular offense which there are grounds to believe has been or will be committed, and direct the acquisition of a particular communication which there is cause to believe will be made in connection with that offense. And it may be thought at first glance that the strict requirements of particularity obviate the danger of a "general warrant." On closer inspection, however, the language becomes ambiguous or worse. I think the ambiguity inheres in the term "particular offense" used in the context of a future occurrence. If the future offense is known in advance with respect to its *facts*, that is, if the court and applicant can predict criminal behavior, the order to seize the evidence of it when it transpired would comport with the Constitution and my fears of "strategic intelligence" gathering are stilled. Where, however, the future criminal activity is predicted only by its particular legal definition (e.g., the crime of "bribery," for example, rather than a particular payment to a particular person for a particular purpose), impermissible general surveillance is the result. I would, therefore, try to clarify the particularity requirement, strengthened perhaps by an express exclusion of general searching, to bring the Act into conformity with the Constitution and to serve notice on those who would employ it for strategic purposes. I hope in this regard that no serious violence is done to the original intent of the draftsmen whose comments in the history of the bill allow some room for doubt.

"Type of communication"

Another aspect of the requirement of particularity is the description of the evidence sought by the search. For many, this is the major sticking point in the effort to insert electronic eavesdropping into the framework of the Fourth Amendment. I do not regard it as impossible to describe with constitutional particularity oral evidence before it is uttered. But I seriously doubt whether the language of Section 2518 (1)(b)iii adequately instructs the applicant on this element of particularity. He is then told only to supply a "particular description of the *type* of communications sought to be intercepted." The critical word, *type*, is undefined and, presumably, might be satisfied by the single descriptive word, "oral". Things are somewhat improved by Section 2518 (4)(c) which adds the requirement that the interception order specify the "particular offense to which it relates." But even this addition, as worded, falls short, I think. The essence of the matter, of course, is that the direction to the police must be sufficiently clear and exclusive to allow him to recognize the communication sought and to reject all other interceptions with a minimum of judgment and discretion. Thus I believe that the Constitution requires a prediction of the contents of the communication—not verbatim, of course but in substance.

Crime list

I understand that before this Commission, as elsewhere, a major issue has become the listing of crimes the investigation of which may be pursued by eavesdropping. Particularly Section 2516(2) directed to state and local governments enables law enforcement agencies (under liberal state statutes) to employ this extraordinary device to gather evidence of the most ordinary and trivial offenses. Although I see some facial ambiguity in whether the felony limitation applies to the enumerated crimes or only to the final "dangerous to life, limb or property" category, the Act seems to have been read to permit a state to authorize electronic surveillance for virtually any investigation. And the reports of the states strongly suggest that interceptions have been made preponderantly in minor gambling cases. For those who expected that monetary exigencies would naturally limit the use of expensive monitors in minor cases, it seems the economics of law enforcement do not obey such inhibitions. Even the most trivial vice investigation, it is said, may lead to a figure of importance in organized crime, and you have to begin

somewhere. Perhaps there is sufficient force and merit to this contention to meet the objections of those who complain about hunting mosquitoes with elephant guns. Yet, I too am offended by the broad employment of this singularly intrusive technique where the immediate quarry rarely warrants serious social concern.

In my original design for the law of New York, I considered the device of enumerating crimes believed serious enough to justify electronic investigation. I rejected it on grounds which I still believe are valid. Simply, a particular instance of almost any criminal conduct may be serious enough to merit eavesdropping, but every instance of the crime in question surely is not. And to enumerate every crime, as Title III does, is of course no limitation at all. My alternative, while flawed, I believe to be preferable. I required that the applicant, being a highly visible and politically responsible official: the chief law enforcement officer of the jurisdiction in question, represent in his application to the court that the matter he was investigating was a crime "of serious significance to the welfare of the community or involves risk of substantial harm to individuals, and that the issuance of the eavesdropping warrant would be in the interests of justice." Although such an averral may not be judicially tested and accords considerable power to the applicant, I thought that the best safeguard against indiscriminate incursions on the liberty of citizens was in the political process itself. Hence, I would have the responsible official stand before his constituents on his record of wisdom and care in the official exercise of his discretion in this matter as he must in the vast and unreviewed areas of prosecutorial discretion generally. I continue to think that the matter of gravity of the matter under investigation must be addressed on a case-by-case, rather than crime-by-crime basis.

Duration and renewal of orders

Another issue of prominence in the debate on electronic surveillance addresses the proper duration of an installation. And well it might, for here the Act is generous to a fault. Although the Act warns that an eavesdrop shall not be in operation longer than necessary to achieve its object, the initial order may remain in effect for thirty days and, whether productive or not, the surveillance may be extended virtually without limit on little more than the original demonstration of probable cause. There is some suggestion in Section 2518(1)(d) that absent special allegations of probable cause to believe that the monitor will be continually productive, authorization terminates upon the first reception of the desired evidence. It is difficult, however, to find elsewhere in the Act a clear statement to the effect that automatic self-termination is the normal and preferred form of an authorization. Moreover, I believe that, in practice, full term orders are routinely sought and routinely granted. In my opinion, this is not as it should be.

Although orders are most frequently obtained in the investigation of continuing conspiracies, it should not be the purpose of the surveillance to acquire all the evidence possible but rather to seek essential evidence only. (Parenthetically, I should say at this point that I fault the Act for its failure to require that the evidence sought be essential to the maintenance of the prosecution for which it is sought, or for the apprehension of the defendant.) Thus the Act should clearly indicate that, absent special circumstances, the authorization shall automatically lapse upon the first acquisition of the evidence sought regardless of what additional, different, or cumulative evidence might be reasonably expected thereafter.

Concerning the maximum time period allowable for the initial request, any choice is of necessity arbitrary. Yet, I must say that thirty days strikes me as unduly long, particularly in light of the generous provision for renewal. I chose fifteen days in my draft, and I am ready to adhere to that figure. I would also limit (perhaps "minimize" is an appropriate word here) the intrusion by advising that normally the authorization should be good only

for certain portions of each day of its life. Most applicants should be able to predict the hours of the day in which the sought conversation is most likely to occur and the Act should require that they do so. Eavesdrop orders should therefore be intermittent as a general rule.

Equally important to the question of temporal overbreadth is the matter of renewals. Regrettably, this is not a subject handled with much care or precision in the Act. Paragraph (5) of Section 2518 discusses extensions, leaving some doubt initially as to whether more than one 30-day extension is allowable. Beyond this ambiguity, (which has not greatly bothered the courts) the provision strongly implies that an extension may be granted largely on the same basis as the original order. Only clause (f) of Section 2518 (1) adds a requirement for the renewal application: the results of the initial monitor must be stated or a reasonable explanation offered for its failure. One would suppose, then, that resubmission of the original application, accompanied by a report of useful interceptions to date or a plausible reason why the lack of them has not dimmed prosecutorial hopes, would suffice to extend the authorization. To me, this spells little short of interminable authority. Surely, time limits have a more important restrictive function than to put the applicant and the complaint judge to the bother of reprocessing papers. As I have already indicated, I would require that no renewal be granted absent some new and additional cause to believe that essential evidence could be acquired during the succeeding term of the order. In other words, it is to be presumed that the probable cause upon which the original application was granted was cause to believe only that the communication would occur within the fortnight following; new reasons should be required to sustain the belief that the monitor will be productive during any other period of time.

Notice

The Constitution itself does not provide for notice of a search and seizure nor for an inventory of the matters seized if any. Yet, as *Berger v. New York* made clear, furnishing such information to the person who suffered the search and seizure has become an important part of the proper execution of lawful search. The matter of notice and inventory is handled in the Act by Section 2518(8)(d), where it is provided that persons named in the order are to receive post-facto notice of the fact, date, and period of the order plus the "fact that . . . communications were or were not intercepted." This minimal requirement may be enlarged by the judge who is accorded discretion to extend notice to other parties to the communications, or to include portions of the intercepted communications. This provision appears to me an unnecessarily and perhaps improperly narrow allowance for notice. With provision for deferral of notice where necessary, I see no reason to deprive all parties to intercepted communications (so far as their identity may be determined) of full disclosure. Further, they should be entitled as a matter of right to receive not only notice of the "fact" that their words were surreptitiously intercepted, but eventually a transcript of the communications intercepted.

Suppression

The Act is unusual in that it incorporates its own provision for a motion to suppress evidence unlawfully intercepted. The statutory description of the remedy however, I regard as inadequate in several particulars. At the very first, the grounds for suppression enumerated in Section 2518(10)(a) i, ii, and iii seem unclear to me. If the first of them does not include the second two, I am at a loss to understand its meaning. I hesitate to believe that hidden in its bland language is some pronouncement on the vital question of whether the motion to suppress will penetrate the face of the supporting affidavit and reach perjurious or inaccurate allegations of fact. Insofar as the statute adds to the conventional lore of suppression motions under the Fourth Amend-

ment, I should like most to have a clear answer to this troubling and uncertain problem.

The same paragraph, para. (10)(a), states the effect of a granted motion but does so in a most peculiar fashion: the contents of the eavesdrop and its fruit "shall be treated as having been obtained in violation of this chapter." If one is tempted by this language to suppose that anything more or different than evidentiary exclusion is intended, the exemption from civil liability in Section 2520 cuts off that consequence. Moreover, the prohibition against evidentiary use embodied in Section 2515 appears to conflict with the consequence of granting a motion to suppress under Section 2518(10)(a). While the latter provision expressly applies to fruit (as it must), Section 2515 mandates exclusion only if "disclosure" would be in violation of the chapter. And Section 2511 decrees disclosure to be a violation only if the person disclosing knows or has reason to know that the source of the information was an unlawful interception. It may therefore be argued that a witness whose evidence was obtained by exploitation of an illegal interception may testify nonetheless if that witness neither knows nor has reason to know that motion was granted suppressing the evidence as the product of an illegal interception. This result, I confess, is so absurd and unlikely that it does little more than point up the awkwardness in drafting of the several provisions dealing with suppression and the exclusion of unlawfully acquired electronic evidence.

Surreptitious entry

The Act as it stands contains no provision specifically authorizing executing officers to make secret entry upon premises for the purpose of installing, moving, or removing an electronic sensor. Some eminent commentator, while seeing no constitutional infirmity in the use of hidden microphones as such, strongly condemn the clandestine physical entry required to place the instruments. While I do not share this view, I do believe that surreptitious entry into private premises constitutes an event of some significance. Hence, I would strongly advise that the law provide that in any case where such entry is required to effectuate the authorized interception, the court be informed of the manner in which the entry is proposed to be accomplished and the location selected for the device. The Act should then direct that the court specifically authorize in the warrant the appropriate and limited physical intrusion necessary.

Emergency installations

I have no quarrel with the emergency provision of Section 2518(7) as such. I believe that there may be occasions when an immediate and temporary eavesdrop is both necessary and justifiable, and the subsequent application for retrospective validation accords sufficient assurances against abuse. However, I do have two quarrels with the section as now formulated. The first is that the word "emergency" is defined neither in the section itself nor in the definition section. Undefined, it has vast and variable connotations; to law enforcement officers in pursuit of evidence or a defendant, many situations appear to require immediate measures of detection. I do not believe we can afford to leave the choice of using eavesdrops without prior approval to the discretion of officers in their unguided, subjective perception of emergency or necessity. Moreover, I think the term is susceptible of meaningful delineation. Hence a definition should be drafted.

Second, I do not care for the limitation of emergency installation to "conspiratorial activities threatening the national security interest or . . . characteristic of organized crime." On the one side, I regard the two descriptions as vague; on the other I see no reason why an emergency installation is not as readily justified for the detection of unlawful activities other than those which the Act attempts to single out as specially important. Since I would allow eavesdropping only for specially grave and threatening criminal behavior in any event, I would append no super-

gravity requirement to the employment of temporary pre-ordered interceptions.

Acquisition of information other than evidence

Finally, I am more than somewhat mystified by the Act's seemingly exclusive concern with the acquisition of evidence of crime. At least in Section 2516, it appears that eavesdropping is sanctioned only for the purpose of gathering proof of an offense. I can conceive of several equally vital and legitimate purposes. Perhaps most of them might be squeezed into the evidence-of-crime rubric, but I believe they are essentially different and should be expressly and separately sanctioned. I have in mind interceptions authorized to obtain information leading to or facilitating the apprehension of a fugitive defendant, the rescue of a victim, or the location and recovery of deadly devices or substances, or the proceeds of crime. In each instance, sufficient proof of the commission of the crime may be in hand, but powerful concerns command law enforcement officers to act further in the interests of public safety and the protection of person or property. If all other requirements of the law are met, I see no reason why electronic probes should be unavailable to these important purposes.

Thank you.

MR. UVILLER: I don't have, as I indicated, a formal statement. I think it would be straining your patience to hear me at length on any of the matters covered in there. I had intended only to touch on the following subjects which I will mention as subjects, and then I will be perfectly happy, if it pleases the chair, to continue.

CHAIRMAN ERICKSON: Fine. As a matter of fact, if you'd like to continue now and answer Professor Blakey's questions, since the time restrictions I thought we were facing have been somewhat alleviated, we can then go back to your prepared remarks.

MR. BLAKEY: Professor Uviller, what you have to understand is that all narcotics transactions themselves may be generally dangerous and the Kel device is a reasonably effective measure, and therefore it would not be reasonable to require, case by case, probable cause to expect a showing of particularized danger.

MR. UVILLER: I hate to endorse that, Professor Blakey, just because I have difficulty with the act in its requirement particularly in other respects.

MR. BLAKEY: Forget the act. It is not what the Constitution says either, but how should we draft a warrant process for consensuals? The existing act is not drafted for that at all.

MR. UVILLER: I would say there has to be a showing of probable cause to believe that there is danger in this particular transaction. But I do believe that probable cause can be derived from a creditable representation that danger is commonplace.

MR. BLAKEY: Common in this class of cases?

MR. UVILLER: In this class of transactions.

MR. BLAKEY: You know, of course, there is a great argument among circuits, and between New York State and California, for example, in the no-knock area. The New York Court of Appeals held that a class showing of danger of destruction of evidence was sufficient, whereas the Supreme Court of California requires showing of destruction case by case.

MR. UVILLER: There is danger in everything a police officer does. Certainly the breaking and entering as it has been described (I think that is the wrong term by the way, to describe a police officer executing a lawful order), the clandestine breach of private premises for installing a microphone is an activity fraught with danger for the police officer. But merely because it is dangerous does not change the lawfulness of the activity, or of measures designed to enhance safety. Rendering a suspect unconscious at the moment of arrest may reduce danger, but is not acceptable on that account. Rather I should say that probable cause requires a demonstration that the particular circumstances threaten harm of a particular sort to a particular person. Based on prior police experience in similar circumstances, as well as general judicial experience, the remote threat should be screened from the likely harm, the slight from the serious danger.

MR. BLAKEY: The second major area where our hearing record indicates consensuals have been used is in the Osborn-type situation, where an informant comes in and makes an allegation against Tommy Osborn who was at that time, I guess, expected to become president of the Tennessee Bar Association, clearly a leading member of the bar. The informant, Vick, himself, would be fairly described as a "disreputable character." The government could not have said, "Based on reliable information I have received from a reliable informant, etc, and that I believe if Vick is wired for sound and talks with Tommy Osborn relating to jury bribery, etc." Instead, the purpose of sending Vick back was to verify his credibility. They could not have sworn out anything about his credibility before that or said that his information was believable.

If you apply a strict Spinelli-type rule, verification by consensuals could not be used. Would you apply a strict verification rule?

MR. UVILLER: A strict probable cause test as in third-party eavesdropping to a consensual?

MR. BLAKEY: That is correct.

MR. UVILLER: No, clearly not. I think one of the principal purposes of consensual eavesdropping is to verify the story of an inherently suspect or incredible informant, and perhaps one of the best

justifications for the use of body recorders is that purpose.

MR. BLAKEY: So again you'd give a dynamic construction to probable cause.

MR. UVILLER: Yes. But again I would say that insofar as expectations of privacy or legitimate and reasonable expectations of privacy govern the Fourth Amendment, some court supervision, some approval by a judge of police using this artificial transmission device, might be legitimate. But you see, Professor Blakey, I don't want to push that too hard because with that there should have been an order for Vick even if he weren't wired.

MR. BLAKEY: I have a great deal of trouble with *Hoffa* and distinguishing *Hoffa* from *Berger*, and the more I think about it, history alone gives me the reason for saying I must have a warrant in *Berger* and not in *Hoffa*.

Let me go on, though, to, I guess, the last link in the chain of discussion.

I take it from your prepared statement that you have no difficulty, as a matter of principle, in the application of the emergency doctrine, the hot pursuit doctrine, to third-part nonconsensual surveillance.

MR. UVILLER: Correct.

MR. BLAKEY: Am I correct you'd have no problem with a similar rule in the consensual ones?

MR. UVILLER: Correct.

MR. BLAKEY: The cops couldn't get there in time—wire a man and send him in anyway.

MR. UVILLER: Right. I do like the intermediate step of telephone warrants or something approaching a telephone warrant. But I have no quarrel with emergency tapping. I regard that as pretty much of an academic matter, however, because as I conceive of a properly drawn statute, the number of instances in which that would be used would be minuscule.

I regard it as simply an extraordinary emergency device.

MR. BLAKEY: You mean nonconsensuals?

MR. UVILLER: In either instance. It is something which is conceivable, but extraordinary in the true sense. The court in *Katz* couldn't conceive of it at all. Perhaps it is inconceivable. But nonetheless, I see no reason for denying the possibility if true emergency necessity should occur in the future.

MR. BLAKEY: For whatever it's worth, the statistics that the Department of Justice has given us has indicated that their prosecutor approval policy in consensuals indicates approximately 50 per cent of some more than 5,000—since I guess about 1969—had to be approved on an emergency basis. That is, there was no time to get prosecutor ap-

proval. So approximately over half of the consensuals they conducted with the system of prosecutor approval, there was no time to get the approval of the prosecutor.

MR. UVILLER: There is no argument with the fact, but that seems to me odd. What I have seen of the use of wired informants leads me to believe that this is usually a very deliberate and carefully-thought-out plan. It takes some time to wire the person, to instruct him in the use of the equipment and so forth, and during that period of time it is quite possible, it seems to me, to get a warrant.

MR. BLAKEY: Let me explore another question with you.

You have echoed the suggestion made by Professor Greenawalt that all the people overheard be notified, at least insofar as they are identifiable.

Let me raise this problem with you. I raised with Professor Greenawalt the problem of notifying you in such a way that privacy is ruptured between you and your wife or you and your creditors. Professor Greenawalt raised the problem of distrust because you learned the party you were talking to might be engaged in criminal conduct.

Let me raise a third problem with you. For the police or any law enforcement system to give that notification they'd have to set up some sort of filing system. In other words, if they didn't know you and you were an uninteresting character in the investigation anyway, they'd make no effort to identify you, just let you pass.

If I understand your suggestion, what you want them to do is make an effort to identify you. Having made that effort to identify you, I take it you'd go in what is the electronic surveillance index in the FBI, and you'd go in that index for two purposes: First, so you could notice under the inventory procedure; and second, you'd also go in that index so that the government could later respond that you had been involved in an electronic surveillance.

Consequently, the policy that you are suggesting, that is, automatic notice to all identifiable people—and I take the meaning of "identifiable" not only those that you know but those with reasonable effort you can know—would unnecessarily put hundreds, maybe hundreds of thousands of citizens into a central index. Their names would be laying in there.

Do you see any problem here since I take it that a number of citizens would have a reasonable expectation of privacy that their names would not be in government files?

MR. UVILLER: Well, you have the advantage of me there since I have no idea what this central index is like or whether or not it is less desirable to insert him in that index in order to get information out of it.

Frankly, it had not occurred to me that efforts to identify the participants, the anonymous participants, in overheard conversations would be independent investigations of that nature. It simply occurs to me that if something is brought against one of the several known occupants of those premises and microphones installed and recordings of all those conversations

MR. BLAKEY: Those cases are easy, but what of a prostitute's calls involving all her "Johns."

MR. UVILLER: And those who call a prostitute would be unidentifiable callers unless they give their names and addresses and they would not receive notice.

MR. BLAKEY: If they came with identification, give them notice, but you wouldn't make any additional efforts to identify them.

MR. UVILLER: I would say that is right, not any extraordinary efforts.

MR. BLAKEY: The same thing with the gamblers. Maybe hundreds are calling in. The gambler is identified; the player is not.

MR. UVILLER: People calling in anonymously, it seems to me, are not identifiable participants unless the voice is actually recognized.

MR. BLAKEY: There is a difference between the word "identified" and "identifiable." You want notices to everyone who was identified. What your paper says is "everybody who is identifiable."

MR. UVILLER: You are probably correct in calling me on that. I meant "identifiable" but I meant identifiable by use of ordinary knowledge, perception, and intelligence, such as the other occupants who, though not named themselves, are known to be visitors—

MR. UVILLER: Willful blindness, I would say, would be the proper standard.

MR. BLAKEY: Doesn't the *Escandar* problem come in there?

MR. UVILLER: I am not talking about motions to suppress.

CHAIRMAN ERICKSON: I understand. I am just looking at the practical aspects.

MR. UVILLER: I think you are pretty much stuck with *Escandar*. You mean if there is a nonparticipant who is a subscriber to the telephone that is being surveilled, should the subscriber nonparticipant receive notice of all the conversations over his telephone.

CHAIRMAN ERICKSON: That is right. It would bother me very much, and particularly—

MR. UVILLER: My feeling, of course, is that it is those holding the conversation that get the transcript of it, not those who pay the rent on the instrument.

CHAIRMAN ERICKSON: I wonder if we can turn to Professor Remington and get his views since we are going to try to exhaust you on direct examination by both Professor Remington, Chief Andersen, and Judge Shientag.

MR. REMINGTON: Earlier in your statement I think you said in your view the search for physical evidence in the court-authorized electronic surveillance raised basically the same type of issue: Is that a fair statement?

MR. UVILLER: Yes. I said I found a certain strain, but not impossibility.

MR. REMINGTON: As I listened to Ramsey Clark this morning, it seemed to me he was saying two things; One, he was clearly saying that there is a difference. Secondly, he was saying the difference in the physical search under Rule 41 is a transitory thing which may have an impact on the individual, but does so in a limited time frame, and apparently is gotten over relatively quickly. The authorized electronic surveillance has a much more continuing, I think he was saying, impact on society generally, which does not result from physical search. And therefore, he saw the electronic surveillance as a much greater threat to the kind of society which he would like to see in this country than he saw the physical search.

How would you respond to that assertion on his part, if, indeed, that is his assertion?

MR. UVILLER: Well, he is privileged to have some direct associations with those who fear electronic surveillance, I suspect, more than the people that I come in contact with. And I certainly couldn't quarrel with his report as to their feelings.

For myself and the people around me, I suspect we feel it is potentially a greater intrusion on those aspects of our life we'd like to keep private, to have the physical possessions or contents of our offices and homes rummaged through than to have our telephone conversations listened to, which are for the most part rather innocuous—if private, nonetheless innocuous.

But mainly I think my problem, as I listened to General Clark, was that the fear, the chill effect of electronic surveillance on freedom and verbal intercourse is largely the fear of illicit or unlawful electronic surveillance. And I don't think he made a clear distinction between those court-ordered surveillances which presumably are limited and brief and based on probable cause and the sort of general intelligence surveillance or illicit, illegal, unlawful, criminal eavesdropping which has caused a good deal of concern.

Many people who are afraid their telephones are being tapped are businessmen and lawyers, perhaps, and others, who are not afraid that law en-

forcement officers are tapping them, but that business rivals or others who may be potential extortionists and others are at work.

I think the chilling effect of electronic surveillance comes in large measure from the technology, from the wonderful world which provides for everybody his own little device to attach to his own telephone and secretly record conversations.

Therefore, I think to a certain extent the paranoia, the unwarranted fear of surveillance and interception is not the product of lawful eavesdropping or statutes authorizing it at all and is falsely ascribed to it.

That doesn't mean to say there isn't some fear. And I have indicated, I think, in my paper, and I'd like to underscore just briefly, that I think electronic surveillance—the act, the law, the statute—is only as good as its limitations and at present I do not think it's sufficiently limited. I believe there is far too much authority, particularly in the hands of state and local governments, to conduct electronic surveillances for what seem to me to be infamous, the gathering of evidence in relatively trivial matters.

And more important—and let me make this point, too—I thought when I first read this act—and I think I have probably said without sufficient thought—that general surveillance, strategic intelligence, is no longer a permissible object of electronic eavesdropping.

Primarily the electronic surveillance carried on by the Federal Bureau of Investigation prior to 1968 was for the purpose of getting information. It was to keep informed.

And I have myself witnessed—and I think it still continues in some quarters—law enforcement officers who believe that it is essential to their function to keep tabs on people, organizations, and activities. And they may be people who are believed to be part of the underworld. They may be people who are believed to be subversives. I don't quarrel with the good faith of these law enforcement efforts, but I do think that the purpose of electronic surveillance is principally that of gathering data and not of getting evidence, and information for prosecution.

It is that kind of general surveillance, that open-ended strategic use of electronic surveillance, that I regard as in sharp contrast with the principles of the Fourth Amendment. To me that is the closest analogue to a general warrant or writ of assistance that could be imagined in the electronic area.

I don't think, now that I have read it more carefully, that the present Title III is clear enough in outlawing the use of electronic surveillance for intelligence purposes. And I think I have

identified—and perhaps not as clearly as I might—I think I have identified the ambiguous provision which allows a law enforcement agency today to stand up and say, "I can particularly identify the crime and show probable cause that this person in the future will commit the crime, and sit on the tap until he commits it." That, to me, is general intelligence eavesdropping that should not be permitted. But I know the argument is made that it is tolerated by the act.

I think the use of electronic surveillance should be limited to crimes of unusual gravity with immediate danger of a serious sort, and for a limited period of time, but more importantly should be limited to the expectation of a future crime which can be identified according to its facts, not according to its generic type.

I am not permitted to sit here on my wiretap until the crime of bribery takes place. I have not identified with particularity the crime if I say it's bribery. It seems to me I should have to say who is paying the money to whom before I have limited it with particularity.

MR. REMINGTON: In your view is the risk of abuse which you have identified as a matter of concern, greater or less if there is narrowly prescribed authority to conduct lawful electronic surveillance? In other words, given the choice between outright prohibition and the way you would like to see it limited—in which of those two situations is there more likely to be impermissible, unlawful, electronic surveillance?

MR. UVILLER: Well, as I regard abuse, I would say that there was a great deal more abuse before 1968, before the enactment of the statute. I think one of the achievements of the Congress was to enact the statute to bring electronic surveillance within a regulatory scheme. Before that, I am sure it was abused, unregulated, unguided, and I assume, in that sense, deplorable.

I tend to believe—I mean it is my faith that most prosecutors, and indeed a good many investigative agencies, try in good faith to conform to the law as they understand it. I am a great believer in clarity and specificity in a statute such as this because I think the clearer you are, the more likely you are to get conformity.

This is not the case of a police officer in hot pursuit. This is an instance in which the chief prosecuting officer of a jurisdiction must vouch for the activity in advance. I think they must read the statute very carefully, and I think they will try to comply. I think if you will give them limited authority, circumscribed, the possibilities of abuse will be reduced.

MR. REMINGTON: I think one other argument that was made in the direction of supporting the proposition that a physical search is quite different from an electronic surveillance is the argument that whereas the physical search raises only Fourth Amendment types of issues, the electronic surveillance also brings up First Amendment issues, and therefore they ought to be dealt with quite differently, and that they do not, in fact, raise issues of a similar nature with regard to liberty; that the freedom to express ideas is qualitatively much more important to a democratic society than the freedom from unlawful intrusion, however important that may be.

I take it you don't feel that difference, to the extent it exists at all, is sufficiently important in your view to cause you to conclude that they are entirely different.

MR. UVILLER: Right. I am no expert on the First Amendment, but I must say I always thought it was directed to public speech and publishing of things, rather than private speech between two individuals in a secluded circumstance.

I agree that the verbal expression in speech, like written expression of ideas, is a matter of special concern. The Supreme Court has more or less disentangled an overlap between Fifth and Fourth Amendments in this special area, and I think the search for written evidence is regarded as being a Fourth Amendment problem entirely. And insofar as the search for written evidence is Fourth Amendment only, it seems to me the search for words in otherwise private circumstances is a Fourth Amendment problem too. I don't believe the absolute language of the First Amendment troubles this analysis greatly.

MR. REMINGTON: Shouldn't the effort to have a statute which narrowly proscribes the authority—do you see an alternative to merely listing the crimes? Is there a more effective way of limiting the authority?

MR. UVILLER: Yes, that is one of the items I wanted to say a word on myself.

As you indicated in your question before, the listing of crimes as the means for expressing legislative judgment on unusual circumstances is very unsatisfactory. It is not only the fact that this act has been reduced in effect to a shambles by the broad scale authorizations to states to name virtually every crime on their books with the possible exception of fornication and adultery as crimes sufficiently serious to justify the use of electronic surveillance. It is also the fact that while certain legitimate targets of electronic surveillance may be engaged in trivial crimes, not every instance of the commission of that crime by any person would jus-

tify electronic surveillance. It just simply cannot be that the unusually grave and threatening conduct, criminal conduct, can be identified by the name of the crime it represents.

Consequently, when I drafted the law for New York, I did not list crimes, nor did I even list crimes by gravity. We thought for awhile instead of the names of the crimes we'd say any crime punishable by over five years in jail is sufficiently serious to warrant it. The Rackets Bureau came back and said many people we think are serious criminals are committing crimes which were not punishable by over five years in jail.

So what we did I don't vouch for as a more effective means, but we chose instead administrative self-restraint by which the administrator becomes publicly accountable. And that is, we require that the chief law enforcement officer of the jurisdiction, who was the only permitted applicant, must vouch to a court in his application that the particular matter under investigation, whatever the name of the crime might be or how serious it was, was a matter which, for identifiable reasons, was of unusual public concern, gravity, or potential harm; and that in that case, in that instance, the ordinary means of investigation being unlikely to succeed, unusual necessity being present, electronic surveillance would be justified.

That is not the kind of a thing which is easily supervised by judicial review. It may be you'd have to have the concurrence of the issuance judge and the local prosecutor that the particular case is one which is sufficiently serious to warrant electronic surveillance, but even that judgment is hardly subject to review and might well become a rubber-stamp approval.

Yet, it seems to me so much the prosecutor does in the exercise of discretion is potentially intrusive, abusive, violative of individual freedoms or otherwise publicly unacceptable, that it is not unreasonable to add this to the list of discretionary choices for which he becomes—at least theoretically—politically accountable.

If he has exceeded what the community tolerates, if he is identifying crimes as unusually serious and matters of great public concern which the community thinks are trivial, then it is political.

And perhaps I am spoiled by my own experience in what I conceive to be a first-rate prosecutor's office, but it seems to me one does not lose in the long run by putting a public official, particularly an elected public official, on his own authority with respect to judgment such as public need or seriousness or threat. This is a customary ingredient of prosecutorial discretion, and it seems to me where it is publicly averred in a document of this sort

prosecutors will think carefully about the use of it. (Inaudible).

Again, I don't vouch for it. But it seems to me it is preferable to what is an artificial and obviously empty restriction in the catalogue of crimes which is presently part of Title III.

CHAIRMAN ERICKSON: Any further questions, Professor Remington?

MR. REMINGTON: No.

CHAIRMAN ERICKSON: Chief Andersen.

MR. ANDERSEN: Continuing with the issue of the seriousness of crimes and their listing you were just talking about with Professor Remington, what is wrong with using wiretap on "trivial crimes in local jurisdictions?"

MR. UVILLER: Well, as I indicated, I do think electronic surveillance is potentially, perhaps actually, the most intrusive form of evidence-gathering in the lexicon. And I would severely limit it to cases of urgent necessity, where essential evidence is to be acquired of a serious crime, or some other emergency requires it, such as the recovery of a dangerous substance, the recapture of a dangerous criminal.

This act seems to speak entirely of the use of electronic surveillance for the purpose of obtaining evidence of crime. It seems to me that is not a sound limitation. There are authorized uses of electronic surveillance for other purposes deemed to be at least as important from the social standpoint. But, always, only where it is the only technique available for that purpose and a demonstration can be made that the matter in question is one of grave public necessity or threat.

MR. ANDERSEN: I have been hearing for decades that law enforcement is basically a local problem. My question is: Unless it is against the Constitution, why should anybody set the priority other than the local law enforcement?

MR. UVILLER: As I view it, it is because the Constitution is one of general application today. It has been since 1961 with respect to the Fourth Amendment, and I think limitations are required by the Fourth Amendment. Therefore, it seems to me Congress has the responsibility of defining those limitations.

MR. ANDERSEN: Do you think there is a level of invasion of privacy from wiretapping geared to the seriousness of crime included under the Fourth Amendment?

MR. UVILLER: Yes, I do.

MR. ANDERSEN: I am the only non-lawyer in the place, Professor. Then a search warrant could have the same criteria, that you could only use a search warrant on certain levels of crime.

MR. UVILLER: On certain levels of crime?

MR. ANDERSEN: Yes, that you could not use it on a \$100 burglary, but on a \$5,000 stick-up man?

MR. UVILLER: I don't know that that has ever been proposed, but I suppose Congress could enact limitations on the search warrant.

MR. ANDERSEN: Isn't that what you are saying on the wiretapping?

MR. UVILLER: Yes, I suppose I am in the sense I am saying electronic surveillance is a variety of search and seizure, but it is a variety of search and seizure of peculiar significance and importance from the constitutional standpoint. It is not conventional. It is not search and seizure which has been time-honored. It is one which requires special limitations and sanctions.

MR. ANDERSEN: I find a conflict in your testimony. In principal 4 you say Congress should not delegate to the states the composition of an unlimited list of crimes, but back in your definition of who should make the choices, you go very heavily to the prosecutor making the choice.

I simply find this is a conflict in thinking.

MR. UVILLER: Oh, I didn't intend they should list it because Congress could not. I don't suggest that at all. I suggest that Congress should not list crimes because that is not a very good way of limiting the use of electronic surveillance. There are better ways of doing it.

MR. ANDERSEN: Then the states should have unlimited rights? Or they, in turn, should limit these state and local prosecutors?

On page 9 you state the individual prosecutor should make the decision of what he wants to use it on. As all local jurisdictions have different sets of priorities, hopelessly different sets of priorities—

MR. UVILLER: I believe those priorities should govern.

MR. ANDERSEN: Even if a trivial thing is first?

MR. UVILLER: Yes, because it won't be trivial under the local requirement. It seems to me the local prosecutor and the local courts should be enjoined to use it in a very restrictive fashion and only for serious and grave threats. However, what constitutes a serious threat, what is a first-priority matter, should be a matter of local guidance. I see no problem there.

I don't think the Constitution enforces uniformity in that regard. For example, it may be a first-degree felony in Iowa to misbrand a steer, whereas in Manhattan it might be a Class B misdemeanor, with no offense to the constitution.

MR. ANDERSEN: I have no more questions.

CHAIRMAN ERICKSON: Judge Shientag.

MS. SHIENTAG: I am also troubled with your suggestion that the chief law enforcement officer of the state decides what crimes merit social concern and therefore should be subject to wiretap.

You were drafting a New York State law where the prosecutors are generally elected in the area of chief prosecutor.

In some jurisdictions, notably the Federal, of course, the chief prosecutor is an appointive official.

Would you amend that suggestion, since the responsibility of going to the voter does not exist for the appointive personnel?

MR. UVILLER: No, I would not amend. Of course, most local ones are elected, but even those appointed on the state level are highly visible, and they are appointed by an official who is himself politically responsible. So it seems to me the political process insofar as it operates in these cases at all operates as well for a high public official who has been appointed as it does for an elected official.

MS. SHIENTAG: So the Attorney General would be responsible for the acts of the U. S. Attorneys throughout the country.

MR. UVILLER: Right. Well, the President would be, the Attorney General not being elected either.

MS. SHIENTAG: So then we'd have to go right to the President on the act of U. S. Attorneys applying for a wiretap?

MR. UVILLER: I honestly think that does have an extraordinary effect. Mind you, all of this is rather theoretical. I am not at all sure a judge is any more responsible in the way he reacts to a search warrant application if he is elected than if he is appointed. And perhaps accountability is only theoretical in any instance.

MS. SHIENTAG: To make it brief because we are almost at 5:00 o'clock, you were troubled with the same problem we are troubled with. What crimes should be included. You were here today listening patiently. Somebody had suggested it not be crimes that were felonies for which the penalty is a year and a day.

We have that problem and it is one that we are trying to wrestle with. Is there any other suggestion that you could make?

MR. UVILLER: That is the best I could do. The listing of crimes or the listing of gravity of crimes I find totally unsatisfactory as a criterion for the use of electronic surveillance. The only thing I can see is a case-by-case decision by responsible officials.

MS. SHIENTAG: Doesn't that leave too much responsibility to the prosecutor?

MR. UVILLER: Under the present act they can get a warrant for any crime at all, with no averral of gravity.

MS. SHIENTAG: Isn't the cost of the listing of one of the deterrents? The actual financial cost cannot be borne in every case.

MR. UVILLER: One would have thought so, but looking at the statistics and the crimes for which it is being used in New York and New Jersey, it appears that law enforcement does not obey those basic economic rules. And eavesdropping is widely used for trivial crimes for which the state gets no return at all.

MS. SHIENTAG: Thank you very much for your patient testimony.

CHAIRMAN ERICKSON: Professor, wouldn't the prosecutor's decision as to what would be a serious crime be binding on the judge under your New York test? Supposing the prosecutor prepared an affidavit setting forth the conclusionary language that you included? Wouldn't that be binding on the judge?

MR. UVILLER: In fact or in law? In fact, probably so. I doubt very much a judge would say, "No, it is not a serious crime." But a law could be written—

CHAIRMAN ERICKSON: I was asking about the New York law. That is a conclusionary statement.

MR. UVILLER: It is more than a conclusionary statement.

CHAIRMAN ERICKSON: But that type of statement is the type that has been condemned in search warrants for years.

MR. UVILLER: Of course, we don't have that problem of gravity in search warrants, do we?

CHAIRMAN ERICKSON: No, but just the language—

MR. UVILLER: Mind you, probable cause would have to be supported. The particularity would have to be very clear and well-defined.

CHAIRMAN ERICKSON: To go into just a couple of other matters before we recess, the annual report that has been filed since the Title III provisions came into effect—do you find that could be improved upon by amendment to the statute to make it more informative?

MR. UVILLER: I am afraid I'd have to pass that one, too, Mr. Chairman. Like Professor Greenawalt, I haven't read the reports themselves, but only comments on them.

CHAIRMAN ERICKSON: Well, I certainly want to thank you on behalf of the Commission for your testimony, your very lucid thoughts, and for the help that you have given us in meeting a very difficult task.

This Commission stands recessed until tomorrow morning at 9:30. We will reconvene in Room 1318, at which time we will be given the privilege of hearing the testimony of Professor Lapidus and Professor Schwartz.

[Whereupon, at 4:55 p.m., the meeting was adjourned, to reconvene at 9:30 a.m., Wednesday, June 11, 1975.]

Hearing, Wednesday, June 11, 1975

Washington, D. C.

The hearing was reconvened at 9:30 a.m., in Room 1318, Dirksen Senate Office Building, William H. Erickson, Chairman, presiding.

Commission members present: WILLIAM H. ERICKSON, Chairman, G. ROBERT BLAKEY.

Staff present: KENNETH J. HODSON, Executive Director, MILTON STEIN, Esq., MICHAEL LIPMAN Esq., MARGERY ELFIN.

PROCEEDINGS

CHAIRMAN ERICKSON: Good morning, ladies and gentlemen.

This meeting stands reconvened.

We are honored this morning to have two of the foremost experts on electronic surveillance as witnesses.

Our first witness is Professor Edith J. Lapidus, Professor of Constitutional Law at Queens College of the City University of New York. She is an attorney, Doctor of Law, student of political science. She is the author of the scholarly work, *Eavesdropping on Trial*, which contains a foreword by Senator Sam J. Ervin, Jr., published by the Hayden Book Company. I believe this is the latest of the publications on eavesdropping.

Professor Lapidus, we are awfully glad to have you with us and we appreciate your accommodating the committee's tight schedule.

Would you be sworn?

[Whereupon, Edith Lapidus was duly sworn by the Chairman.]

TESTIMONY OF EDITH J. LAPIDUS, PROFESSOR, QUEENS COLLEGE, CITY UNIVERSITY OF NEW YORK

CHAIRMAN ERICKSON: You have been kind enough to answer a questionnaire that we sent to you. Do you have any opening remarks that you would care to make?

PROFESSOR LAPIDUS: Yes, Mr. Chairman and members of the Commission.

I appreciate this opportunity to appear before you and to discuss the problems, the many problems, of law and practice involved in the operation of Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

I did prepare a statement, a rather brief statement, which supplements the answers to the questions in your questionnaire, and I would like to read this statement to the Commission and also to put it on record.

I do have a more detailed statement prepared much less hurriedly and at greater length, which I prepared for the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the House Committee on the Judiciary. That appears in hearings of the Subcommittee dated April 28 of 1974, just a little over a year ago.

In the statement to the House Subcommittee I treat many of the same questions that have been troubling this Commission, and I summarize them in my proposals, both as to law and practice.

Both of these statements are based on the analysis and evaluation of law and practice on Federal and State electronic surveillance that eventually took the form of my book, *Eavesdropping on Trial*.

I want to emphasize the fact that in this book I made a great effort to be impartial, objective, unbiased. And, as you know—I am sure all the members of the Commission realize—that that is not easy, because we all seem to have some predispositions on the subject. And that naturally is so because there is a built-in conflict in the problem between the right of privacy and the legitimate needs of law enforcement. We have no better way—there is no other way—of approaching the problem than to balance the equities.

Some of us are more concerned with the right to privacy and others with the needs of law enforcement, and some of the views of each of us depend on past experience.

The law enforcement people are likely to think that the needs of law enforcement come first, and the people who are involved with constitutional liberties, as Senator Ervin and I have been—since I teach Constitutional Law and give a seminar on the Supreme Court—we are concerned constantly with erosions of civil rights and constitutional liberties. We are inclined to think that maybe things are out of balance.

I have made an effort in my study, to be as objective as possible and in my proposals, too, to make proposals that will not unduly interfere with law enforcement and criminal cases, which is what Title III, of course, is all about.

So with your permission I would like to list my proposals, both in the short statement to the Commission, and in the proposals that I have made before the House Committee, and then perhaps the members of the Commission would like to talk about one or two subjects that have been troubling them.

There are some matters that you have discussed that I did not even consider. I think you go much further than I did, especially in connection with consensual eavesdropping, which I never thought that we would undertake to place under the provisions of court-ordered requirements. Perhaps we want to talk about that.

There are one or two aspects of wiretapping that were not discussed yesterday. The discussion was so full and able, that I am not sure I can add much to it. But if I can, I would be happy to do it.

So with your permission I would like to read my proposals.

CHAIRMAN ERICKSON: I judge you will file with the reporter your statement for the record?

PROFESSOR LAPIDUS: That will be fine. They will both be made a part of the record in this proceeding.

PROFESSOR LAPIDUS: I would like to read them now to indicate what matters have had my most serious consideration, so that you can select from among those what we should talk about this morning.

First: "To limit the covered offenses to serious crime."

What troubles me is that this law, Title III, was intended to deal with the problem of organized crime and serious crime. But from my study, it seemed quite clear that while law enforcement people would have liked very much to attack organized crime and serious crime they haven't made much headway. Especially at the state level, the law has not been used for serious crime. It has been used against small-time gamblers. It has been used against small-time dealers in narcotics. Gambling and narcotics account for about 80 per cent of the court orders.

Law enforcement officials are not happy about it. They would like to get to the top echelon people in gambling and narcotics, but in many cases are not able to do it. They are frank to say they will use the wiretapping law wherever they can to catch criminals, and if they happen to be low echelon, that is too bad.

I feel we should be able in some way to limit the covered offenses, to indicate clearly that it should be used only for serious crime.

One of the witnesses—Mr. Greenwalt, I believe—suggested that perhaps this is an administra-

tive problem. No, it was Professor Uviller who said perhaps what the Commission should do is to urge the law enforcement officials to use restraint.

Now, that is very good. I think that certainly they should use restraint. But I do not think that that is enough. And I think a skillful draftsman of legislation could figure out how we could, especially at the state level, impress on state officials that electronic surveillance is a tool that is highly intrusive of privacy, unavoidably intrusive. It is subject to great abuse.

Of course we do not know to what extent it has been abused. We do know from court cases that it has been abused to some extent. Law enforcement officials have to be impressed with the fact that this is a dangerous tool, that it was never intended to be used for petty offenses.

My second suggestion is—and this was not touched on by any of the witnesses yesterday, and I think probably it did not concern them because they did not do what I did—go around to the law enforcement people, the District Attorneys' offices, the judges, and others—all the officials who were concerned with applications and orders—

I would like to suggest that the Commission urge the Congress to make progress reports to the judges mandatory.

At the Federal level, I believe that the Federal judges are asking for written reports; that is, in their orders they require that progress reports shall be made at certain intervals, and that is their practice.

At the state level, not only does the order not require the progress reports, but very often no progress reports are made. I interviewed several judges who confirmed this.

CHAIRMAN ERICKSON: Professor, I wonder if you could hold that microphone just a little closer.

PROFESSOR LAPIDUS: I'm sorry. I can talk much louder.

CHAIRMAN ERICKSON: You are coming through loud and clear.

PROFESSOR LAPIDUS: Is that better?

CHAIRMAN ERICKSON: Much better.

PROFESSOR LAPIDUS: Good.

At the state level I talked to several judges. Judges are very conscientious, and the law enforcement people are very conscientious, too. They are anxious to comply with this law, but some of them do not understand the law very well. And, again, I am talking about people at the state level. Federal judges are also much more aware of the dangers of not complying with the statute.

In the case of the states, one judge said to me, "Oh, yes, so and so"—the District Attorney he is used to working with, the District Attorney who brings these applications to him—"I guess he comes

up to my office every now and then and tells me how he is getting along."

Well, that is not good enough for compliance with the law. The order should require that progress reports be made at regular intervals so that the judge knows exactly what is going on.

CHAIRMAN ERICKSON: If I may interrupt you there, you have dealt with the period of time over which the order can extend. What do you think would be the proper time that should be made the subject of this electronic surveillance order?

PROFESSOR LAPIDUS: I feel that 15 days as the maximum is adequate.

The reason I say 15 days is that most of the Federal orders call for 15 days.

I noticed in the last report to the Administrative Office of the United States Courts, the report for 1974, that in quite a few cases they asked not for 15, but for 20.

So while I would have said that 15 is certainly ample—if it is enough for the Federal people, it should be enough for the state people—now I am beginning to wonder why all of a sudden they are asking for 20 days.

When I interviewed them—my book, *Eavesdropping on Trial*, came out in February 1974 and took about a year to go through the press—at the beginning of 1973 the Federal people were telling me that a period of 15 days is ample. And if you ask for 15 days and intercept wire and oral communications more than 15 days, then if that is tested in the courts it is not going to look very good. It is going to look as though you have been going on a fishing expedition.

I think it would be fair to say that 15 days should be a maximum. That was one of the questions—yes, that is number 4.

CHAIRMAN ERICKSON: Let's explore this if I can go forward just one minute.

PROFESSOR LAPIDUS: Yes.

CHAIRMAN ERICKSON: If, say, the order was 15 days, in making progress reports within that 15-day period what do you think should be the time for the first progress report?

PROFESSOR LAPIDUS: Five days. Divide it into three periods.

As the law enforcement people explained it to me—now, of course, I never was a chief of police or any kind of police; I never was a law enforcement official—what the law enforcement people say is that if you don't get it within a few days, then you are on the wrong track. That isn't always true, but generally that is true.

CHAIRMAN ERICKSON: All right, now let's take the fact that you are just elucidating on.

At the end of the first five-day period the progress report comes in and it has produced just what you have suggested—nothing. What should the judge do at that point?

PROFESSOR LAPIDUS: Well, at that point the judge at least would have an opportunity to talk to the law enforcement official, and he would have to reassure him that this was the kind of case where perhaps something would come through in another five or ten days.

CHAIRMAN ERICKSON: All right.

PROFESSOR LAPIDUS: At least the judge would keep his finger on it.

CHAIRMAN ERICKSON: All right. At the end of the five-day period there has been no reason to believe that any illegal activity is going on. Should the judge dissolve the order at that point, or dismiss the order?

PROFESSOR LAPIDUS: No. There I would say no. You have the 15 days and the law enforcement person is entitled to that 15 days.

But the point is that when you have to report to a judge, you are not likely to keep on tapping when you already have the information which you say you wanted.

CHAIRMAN ERICKSON: But if the progress report is going to have the maximum impact, if it was unproductive, shouldn't the order be quashed?

PROFESSOR LAPIDUS: No, I don't think so. You see, the progress report has two functions. It serves as a check on the law enforcement official who is apt to get a bit overzealous.

He has his information, but it is so nice to get a little more.

I think it is the judge who should say—let's take a different kind of case, not a case where you get nothing, but a case where you really have something.

CHAIRMAN ERICKSON: Let's follow this one where they got nothing.

At the end of ten days they come in on the second progress report and they still don't have anything.

PROFESSOR LAPIDUS: Well, at that point the law enforcement official will have to be a little more convincing, but I would say he still has his 15 days. But the record would show that he has made this report to the judge and he knows that he has to report.

I think of the progress report not only as a way of limiting the time in effect, but I think of it as a deterrent to keeping it on an excessive amount of time.

CHAIRMAN ERICKSON: Now, at the end of 15 days, the law enforcement officer comes in and he says "We haven't done anything yet, but we really

think we are going to get it so we would like a 15-day extension."

PROFESSOR LAPIDUS: Well, there I suggested a ten-day extension.

CHAIRMAN ERICKSON: Then he grants him a ten-day extension and at the end of the five days, which would be the next progress report, he comes in and he still doesn't have anything. What should the judge do?

PROFESSOR LAPIDUS: Well, this all depends on the circumstances. Every case is different. I should say that he should have his ten days.

It just couldn't happen that way. You really have to talk to some of these law enforcement people and the judges to see how they work together. They *have* to work together.

CHAIRMAN ERICKSON: I understand exactly what you are saying there. I will ask this: In your experience, have you found that the New York judges scrutinize the progress of a wiretap?

PROFESSOR LAPIDUS: I do not like to make public comments about the New York judges. One of the judges whom I interviewed was forced to resign, so I had better not talk about any others.

There were no progress reports that were of any account at all that I could find.

CHAIRMAN ERICKSON: All right.

Now, if I can take this opportunity to digress on one point, you have examined in depth the Administrative Office of the United States Courts Report on application for orders authorizing or approving surveillance of wire or oral communications?

PROFESSOR LAPIDUS: I have looked very carefully at the reports. The most recent report came to me just a few days ago and so I haven't read this one very carefully, but I have seen it, yes.

CHAIRMAN ERICKSON: You have seen the others?

PROFESSOR LAPIDUS: Oh, yes, I have studied the others very carefully; yes.

CHAIRMAN ERICKSON: From your review of these reports, do you feel that they fairly and accurately fulfill the function that was intended by the filing of such a report, or do you feel there should be amendments to the statute to require more definitive reporting, to require more detail, require more facts—something that would cause the report to flesh out a little bit?

PROFESSOR LAPIDUS: Yes. There are three reports and maybe we should take each one separately.

CHAIRMAN ERICKSON: All right.

PROFESSOR LAPIDUS: There is the report by the judge, which has to be filed within 30 days after the termination of the interceptions.

Then there is the annual report that has to be filed by the prosecuting officials on each wiretap or electronic surveillance.

And then there is this statistical report to Congress by the Administrative Office of the United States Courts.

All three reports serve a very useful purpose. They all give information that Congress should have, that the public should have.

There are however, several difficulties with the reports. Let's take the judge's report first.

There was no judge that I talked to who had a kind word to say for the report because, to him, it was just a nuisance to have to fill out. And most judges did not even do it themselves.

Again I am talking about the state level. Federal judges do not have as many orders so it is not such a nuisance for them.

CHAIRMAN ERICKSON: You are not basing your comments about whether the Federal judges fill out their reports on actual contacts with the Federal judges?

PROFESSOR LAPIDUS: I am not talking about filling out accurately—

CHAIRMAN ERICKSON: Not accurately—whether they fill out the forms or whether somebody does it for them, whether the clerk does it as a routine matter.

PROFESSOR LAPIDUS: Well, of course I would not know that.

I do know that in New York, in some of the counties, it is routine; it is not done by the judge; it is done by the law enforcement official and then it is just sent up to the judge for his signature and he puts his signature on it and that is the end of it.

So far as the law enforcement official is concerned, I went to the Administrative Office of the United States Courts and after much cajoling and pleading and asking to see the reports, themselves, I did see quite a few of the reports.

One of the things that I noticed on the report was that there is a place at the bottom of the report which asks that the law enforcement official assess the value of that wiretap. That information, in most cases, was left blank.

CHAIRMAN ERICKSON: Let's follow this point up.

Supposing the barest of information is included—and in fact it would be what would often be characterized as a skeleton report, where no more than the limited information required by the statute is included—or perhaps not even that amount.

What is the sanction that can be imposed against the state for failure to file the report?

PROFESSOR LAPIDUS: Well, I don't know. There are sanctions in the law, itself, which says that you must comply with the law. And they do comply.

The Administrative Office doesn't do anything if someone doesn't comply.

CHAIRMAN ERICKSON: That is the point I am making.

PROFESSOR LAPIDUS: Yes. Well, that is a matter of enforcement. The Administrative Office tries to get the report—

CHAIRMAN ERICKSON: Supposing the state just doesn't file anything. The law specifically requires that the report be filed, but they elect not to file. Then what?

PROFESSOR LAPIDUS: Then I think they have violated the law and somebody has to take the initiative to prosecute.

CHAIRMAN ERICKSON: If they violate the law and fail to file the reports that are required, should they be able to continue to utilize the statute for wiretapping and electronic surveillance discovery purposes?

PROFESSOR LAPIDUS: I don't think that you would have to go that far. There has not been that amount of laxity.

What does happen is that when somebody files a form that is incomplete or does not send any form in, the Administrative Office simply writes and asks for the additional information or for the form, itself, and usually they get it.

After all, it isn't such an effort. It is a one-sheet form. One district attorney says he spends 14 hours in a day to fill them out. But actually I don't think it takes that much time.

So I don't think that is the problem. I think they have been filed.

CHAIRMAN ERICKSON: Do you think the forms should be more complete? Do you see any additional items that should be an additional subject of inquiry?

PROFESSOR LAPIDUS: Yes. In one of the statements that I submitted to the Commission I do list the weaknesses of the form. The report to Congress reflects the weaknesses in the reports by the judges and the prosecuting officials, because all it is a statistical report that collates the information.

So, may I read to you what I felt were the weaknesses in the report?

I list, for one thing—this is in the report to the Administrative Office—the average frequency of intercepts per day.

This is supposed to give us an idea of what you get each day.

Now, that, I think, is quite meaningless and I give an example.

Suppose during a 30-day period you get no interceptions until the 30th day, and on that 30th day you get 30 interceptions.

What is the average frequency? Would you say the average frequency is one? When that report is issued to Congress, it sounds as if you have this 30 days and every day you get one interception.

I think that it is misleading and it is meaningless. There is a lot of meaningless information in the report. What has to be done with the report is to concentrate on giving meaningful information. And the most meaningful information for the report is whether that wiretap was actually used in obtaining an arrest and a conviction, and whether that wiretap was the only way of getting arrest and conviction, whether there was other evidence that was obtainable in some less intrusive way.

That is the only way that you can tell whether a wiretap has really been effective.

The report does not do that. The report has to give a statement only as to whether an arrest or conviction occurred.

It is very possible, and there have been cases where the wiretap was obtained, that the wiretap was completely useless either because the information that came off the telephone was not incriminating or was not helpful in any way; but there was an arrest and there was a conviction. That would count as a wiretap which resulted in an arrest and conviction. There should be some way of making the law enforcement officials tell whether or not it was really effective in producing that arrest or conviction.

I don't know how that could be done. It would be very difficult legislation, I imagine, but it would be worth trying.

CHAIRMAN ERICKSON: If my memory serves me right, the late J. Edgar Hoover took the position at one time, anyway, that the material intercepted in a wiretap or a bug should not be admissible in evidence, but that the material gleaned from the tap should be available for intelligence purposes.

I think most of the authorities recognize that in a great many instances the material that is intercepted does not furnish direct evidence, but that it does furnish leads to other evidence that can be used for the purpose of prosecuting a criminal charge.

Isn't that true?

PROFESSOR LAPIDUS: Well, Mr. Chairman, you are onto an altogether different topic, and that is my No. 7.

CHAIRMAN ERICKSON: I understand that.

PROFESSOR LAPIDUS: And that is the whole problem of whether the law intended that you should be able to get strategic intelligence. And that is a very difficult problem.

Would you like me to talk about that now? Is that what you are asking me? What you asked me is whether I think that Mr. Hoover was right in saying—

CHAIRMAN ERICKSON: Yes, whether or not these taps, in your experience, do produce direct evidence of crime or whether they are primarily of assistance in developing leads to evidence that can result in the prosecution of criminal charges.

PROFESSOR LAPIDUS: Well, my view, Mr. Chairman, is that the law was not intended to permit the interception of communications for the purpose of obtaining strategic intelligence, that it was intended to get specific evidence of a specific crime and not simply to listening in the hopes that maybe you would get leads.

So I can say definitely for myself that I feel that the law did not intend to do that, that there was no authority for it, and if it was so, if the law did permit it, I am not at all sure that it would be constitutional. Because that is in the nature of a fishing expedition. It is in the nature of—well, a general warrant. And that is not what the purpose of this law was.

Does that answer your question?

CHAIRMAN ERICKSON: It does, indeed.

Now, you have expressed views on the consensual electronic surveillance. Do you feel that consensual taps, where we have the wired informer—the *White* case, if you will—

PROFESSOR LAPIDUS: Yes.

CHAIRMAN ERICKSON: Do you feel there should be legislation dealing with this particular aspect of electronic surveillance?

PROFESSOR LAPIDUS: As to that question, until I received your questionnaire I had not given it much thought because, of course, the Supreme Court has sanctioned that kind of eavesdropping without court order. And while it was a 5-to-4 decision, a divided decision, I accepted it. And it never occurred to me this Commission would consider suggesting that perhaps we should have a court order in that type of eavesdropping.

As I thought it over, I felt it would be an ideal solution to stop some of the excessive wiretapping, consensual wiretapping, that has gone on. We know there are tens of thousands of cases every year, and it is a very good way of getting evidence and a very easy way, and I certainly would not like to take it away from law enforcement officials.

But I think it would be a very fine thing if Congress would pass a law to say that even in such cases a court order should be required.

I think especially, at the beginning, that it would be a real hardship for the law enforcement people, but I do think it would discourage excessive use of this method of investigation.

In my report before the House Committee a year ago I said that since the Supreme Court had sanctioned consensual eavesdropping, Congress would not reconsider it. Congress would not consider outlawing electronic recording of conversations without a court order unless there was consent of both parties.

But at *this* point I feel that if the Commission has thought about it, it must be in the air that perhaps it is time we put a stop to so much of this so-called "consensual eavesdropping." It is not only furnishing informants with recording machines; it also involves third-party overhearing of conversations. And there has been a great deal of it.

What troubles me about consensual eavesdropping is that in many cases it has been used as a sort of entrapment.

I know it is not legal entrapment because law enforcement people do not wire informants with recorders to talk to those who are not inclined to commit some kind of crime, in gambling or in narcotics. It does not qualify as legal entrapment. But there is an element of entrapment in it.

You send out this informant and equip him with a recorder, and he is going to talk to this man. Maybe he was not inclined to commit whatever crime he is going to talk about, but once he gets started he is led into it.

I have this uncomfortable feeling about this type of eavesdropping.

CHAIRMAN ERICKSON: Do you feel it would be better to leave both of them to tell their own version of what occurred at that time rather than to have that conversation recorded accurately so it could be reproduced for the jury to accept for its face value?

PROFESSOR LAPIDUS: No, of course the recording is much better evidence than their oral testimony. After all, most of the informants are people who come out of the jails and you never know whether you can believe them or not. But you can believe a recording machine.

No, my thought is that it would be better to require a court order in this type of case. I don't think that would be asking too much.

CHAIRMAN ERICKSON: Such as was done in *Osborn*?

PROFESSOR LAPIDUS: Yes, as it was in *Osborn*.

Of course, we don't know—*Osborn* wasn't very clear as to whether that court order is required, but there was a court order in *Osborn*, yes.

CHAIRMAN ERICKSON: Do you believe that electronic surveillance serves any legitimate purpose in law enforcement?

PROFESSOR LAPIDUS: Oh, yes. It does serve a purpose. If law enforcement people have it, it is just an additional tool.

Let me make my own position clear about the use of wiretapping and electronic surveillance. I was rather surprised when I came down yesterday in a taxi with Chief Andersen and discovered that I had been scheduled with all the opponents of eavesdropping.

I do not feel that I belong in either camp.

Perhaps if we could go back to 1967, when Congress was considering the Right of Privacy Act, where all eavesdropping was banned except in national security cases, I might have felt happy with that law and thought, "Well, that is a good way of protecting our right of privacy."

But now I take a very realistic view of it. We have Title III. We do have sanctions, we have eavesdropping with safeguards. And I think if those safeguards really are respected, if the law is clear and the people who use the law understand what the law requires them to do, that we have achieved as good a balance as we can get between the right of privacy and the need of law enforcement.

It is an added technique, and I, for one, would not like to say to a law enforcement official who has the job of catching the criminals, "Well, here is a wonderful tool but you can't use it."

We have it and I think what we have to do now is make sure it is not abused, to make sure the law is clear.

CHAIRMAN ERICKSON: With all deference to the draftsmen of the law, do you see any ways that this law could be amended to improve it?

PROFESSOR LAPIDUS: Oh, yes. I don't think it is a reflection on the draftsmen at all that the law is not completely clear. I don't know of any law that is completely clear. If any law was completely clear, we wouldn't have any litigation. You can't foresee every contingency. You can't really express any law in language that is so clear that you can't misinterpret it.

It is only as the law is being put into operation that you discover what could be clearer.

I think that in my statement I have a list of matters that I thought could be clarified.

One of the things—and this is a problem which was considered yesterday—is the matter of the notice. I think it is not quite clear as to who should get notice. The law does say that notice is to be given to the person who is named in the order, and to such other persons as the judge shall direct in his discretion.

But then when you define an aggrieved person—and an aggrieved person has a right to make motions to suppress—"aggrieved person" also includes people whose conversation is intercepted.

I think there is an inconsistency there, and I think it could be clarified very easily by requiring that notice should also be given to people whose conversation was intercepted. And that is something that was discussed yesterday, and there were some problems. I believe you raised some problems as to how you identify these people.

But I don't think that is an insurmountable problem, either. The law could say that you give notice to people who can be identified with a reasonable amount of effort—in some cases you can't identify them. But in many cases you can. And it seems to me those people should get notice because they are included as aggrieved persons, so that there is no reason why they shouldn't know just what it is that has been done.

CHAIRMAN ERICKSON: Do you feel that there is a need to provide licensing for the manufacturers of electronic surveillance equipment?

PROFESSOR LAPIDUS: Well, that was one of the questions on your questionnaire and I couldn't see how licensing would help.

I think that so far as private wiretapping is concerned, private electronic surveillance, the law has been a complete failure. And it has been a complete failure because there has not been enforcement.

I discussed that problem with the attorney who is in charge of enforcing this particular provision of the law in the Department of Justice, and he showed me a thick file of correspondence that he had with respect to violations of this provision which says that you can't manufacture and sell electronic devices that are intended primarily for surreptitious eavesdropping.

Now, perhaps there could be found some other way of stating it so it would be so simple to evade.

But as the law stands now, it is very easy to evade the law, and there have been very few prosecutions. When I asked for specific prosecutions, he couldn't think of any but he says there have been a few. At the state level there have been practically none. And the reason is that it is very easy to evade this prohibition. And licensing the manufacturers won't help because the manufacturers are not manufacturing electronic devices and then selling them to private individuals. They sell them to the law enforcement people.

What the private people do is to buy the parts—it was a matter of discussion here yesterday, too—that within a half-hour you and I could buy ourselves some recording equipment without any difficulty, and some high school electronics expert could put it together for us.

So I don't see how licensing manufacturers would help.

CHAIRMAN ERICKSON: Well, how do you see that we could vigorously enforce prohibitions against the use of electronic surveillance material by unauthorized persons, either the police or on the civilian side?

PROFESSOR LAPIDUS: I really can't answer that. That is a law enforcement problem.

The way those cases come to the Department of Justice and to the states is by way of complaints. One manufacturer complains that some other manufacturer is advertising a product which is really an electronic device primarily intended for surreptitious purposes, and he is calling it a toy.

There was a very intriguing one in the shape of a little beetle. They said, "This is a toy." Well, it wasn't a toy. It was a sophisticated electronic eavesdropping device.

All the Department of Justice did was to write to this manufacturer and say, "Look here, we are going to prosecute unless you withdraw it from the market."

So they withdrew it from the market, but of course tomorrow they can produce something else and it could go on and on. So I don't know how that could be done.

But I do think that what can be done is to establish a climate where wiretapping and electronic surveillance are discouraged rather than encouraged, made difficult rather than made easy.

I think the general public has just got the idea, "Well, everybody is doing it, so we may as well do it, too."

And if one person consents and we say, "Well, that is all right, you do not even need a court order for that," that makes it very easy. If Congress provided that you do have to get a court order unless all the parties to the conversation consented, then people would know you can't do all this wiretapping and all this electronic surveillance without proper safeguards.

CHAIRMAN ERICKSON: From your report I judge you feel that the *Rathbun* exception which was drafted into Title III should be modified, restricted, or eliminated to require the consent of all parties?

PROFESSOR LAPIDUS: I think it would be a very fine thing if it could be done. I am not so sure that Congress is ready to do it.

And the reason I hesitated, the reason I didn't even consider it, was that, after all, the Supreme Court has spoken and I am not sure whether it is the Court or Congress who should do this. But I suppose if we require a court order, it would be the function of Congress, and surely the courts would uphold it.

CHAIRMAN ERICKSON: I am very familiar with the *Rathbun* case. That came from our Tenth Circuit and I knew the parties and circumstances.

PROFESSOR LAPIDUS: Oh, yes.

CHAIRMAN ERICKSON: You will recall in that case, Rathbun called and was overheard on an extension phone after certain threats had been made. Now, this is very close to the consensual recording, isn't it?

PROFESSOR LAPIDUS: Yes, it is.

CHAIRMAN ERICKSON: Fairly close?

PROFESSOR LAPIDUS: Yes, it is.

CHAIRMAN ERICKSON: Do you feel that every person has a right of privacy in his conversation over a telephone or his conversation with any other person that can't be violated until you have a court order stating that you can listen in on it? Is that about what you are saying?

PROFESSOR LAPIDUS: Well, you are making it very broad and it is a very hard question. And, as I said before, perhaps on this problem of consensual eavesdropping I have not given it as much thought as I would like.

I do remember one case, not a Supreme Court decision, but in one of the states—I think I give an account of it in *Eavesdropping on Trial*—where in a jail somebody listened—

CHAIRMAN ERICKSON: That is a Washington case, the Supreme Court of Washington.

PROFESSOR LAPIDUS: Yes.

I am really not willing to take a stand on the question of listening on an extension. I would like to think about it a bit more. I know that it was discussed yesterday, and I thought about it for a time, but I haven't made up my mind. Let us put it that way.

CHAIRMAN ERICKSON: The Supreme Court of Washington—and there is a California case on this, too. And I believe they are in juxtaposition. Some of the cases say there is no right of privacy in the jail, that surveillance of the activities of the prisoners is part of the duty of the warden, but it could be a different problem if it was a question of bugging the attorney's conference room in a jail, would it not?

PROFESSOR LAPIDUS: Yes.

CHAIRMAN ERICKSON: There you have a Sixth Amendment right-of-counsel violation.

PROFESSOR LAPIDUS: Yes.

CHAIRMAN ERICKSON: But as far as the right of privacy is concerned, which is essentially what we are talking about, that right hasn't been defined as to how far it goes on a case-by-case basis; isn't that right?

PROFESSOR LAPIDUS: Yes, that is very true. I was very interested in the colloquy you had yester-

day on the expectation of privacy. That, too, is a very difficult problem because what expectation of privacy do we have? It depends on the circumstances.

We pick up a telephone and we expect that it is a private conversation, but maybe it isn't a private conversation. And we know that a great many conversations are overheard. So maybe we have no right to an expectation. We have a right of privacy, but maybe we have no right to expectation.

CHAIRMAN ERICKSON: As you know, the State of Illinois has acted on this consensual eavesdropping area, and they have suggested that law enforcement be limited in their use of consensual eavesdropping equipment to the case where the chief prosecuting officer gives approval.

Would that meet the requirements that you believe are necessary?

PROFESSOR LAPIDUS: I think that would be helpful. That doesn't go far, of course, as the requirement of a court order.

CHAIRMAN ERICKSON: I might ask this: If you were to require a court order, what would you require be shown to justify the issuance of that court order for consensual eavesdropping?

PROFESSOR LAPIDUS: I would say it would be the same requirement as in ordinary cases. You would have to show probable cause. There is no reason why it should be different in that type than some other.

You would still have to meet the requirements.

CHAIRMAN ERICKSON: You would try to restrict that to the four corners of *Spinelli* and *Aguilar*, and so on?

PROFESSOR LAPIDUS: I think so.

CHAIRMAN ERICKSON: Don't we have the problem that was outlined in *Berger* that it is very difficult to predict the parameters of a conversation that hasn't occurred?

PROFESSOR LAPIDUS: Well, of course, now you are touching on a very tender spot. After all, in the application are you supposed to show that you want a particular conversation, or do you only have to show the type of conversation that you want? That is a serious constitutional problem.

And if we get into that, we will have to say that perhaps the whole of Title III is unconstitutional.

In the kinds of cases where wiretapping court orders have been obtained, they have generally been the kind of cases where you cannot say that you want to get a specific piece of evidence. You have to simply indicate the type of evidence that you want.

You can never tell the court that such and such a conversation is going to take place and you want to intercept it because of course you don't know if the conversation will ever take place.

CHAIRMAN ERICKSON: How would you limit the list of crimes for which electronic surveillance may be authorized?

PROFESSOR LAPIDUS: That, too, is a very difficult problem of drafting legislation.

I do feel that perhaps it could be made clear that with respect to gambling—until we legalize all gambling, which would solve at least half the problem—that it ought to be made clear in some way that it is the serious gambling that we are concerned with, that it is serious violations of narcotics that we are concerned with, and maybe limit some of the other offenses.

I think in that case, too, it is the law with respect to the states that perhaps needs clarification more than the Federal, because there is this open-ended provision with respect to the states, where the offense is punishable by imprisonment for more than a year, and it includes crime dangerous to property as well as to life—perhaps that is a bit too broad.

For example, I can conceive of a case—I don't know just what the state laws are—where a state might provide that if somebody is found with the possession of marijuana the penalty is imprisonment for more than a year.

Now, that would bring that offense under the provisions of Title III, so that you would be able to wiretap with a court order.

I think that is going a bit too far. I think this type of intrusion into privacy should not be used for such a purpose. I don't know whether it is ever used in that kind of an offense but it is possible to do so.

I feel that some study should be made of the wording of the offenses listed for the states. It is a very, very broad statement. It is quite different from the provision for Federal wiretapping.

CHAIRMAN ERICKSON: In your answers to the interrogatories that we posed, you suggested centralization of state wiretapping machinery.

How would you effect that?

PROFESSOR LAPIDUS: Well, I really don't know how that could be done. I haven't thought that out. But what I do know is that there are a great many people who apply for court orders and the supervision is not very great.

Perhaps instead of permitting anybody in any political subdivision, that is, in the state government—some kind of local subdivision—there could be incorporated in the state law some kind of supervision so it wouldn't be possible for so many people to apply for orders without any kind of oversight.

That happens in New York; it happens in New Jersey. If you look at the reports of the Administrative Office, you can see how many law enforcement officials have applied. I once counted them up, but

I have forgotten how many there were in New York—a great many.

I can't say how that could be done. It depends on the set-up in each state. But I think in some way there should be greater supervision of the people who can apply for court orders.

CHAIRMAN ERICKSON: You have suggested that we limit wiretapping to the more serious crimes?

PROFESSOR LAPIDUS: Yes, I think it should be limited to serious crime.

CHAIRMAN ERICKSON: Let's assume that we were investigating a gambling charge that was alleged to be of monumental size, that is, involving many people and millions of dollars in operations.

So the tap is authorized. The tap is put in. The progress report is made that you have mentioned, and it turns out to be the "Ma and Pa" type operation that is often referred to, and doesn't indicate a gambling operation of anything but the most insignificant size.

Should the judge then dissolve the order?

PROFESSOR LAPIDUS: Now, let me say that I personally think that this law should not be used in gambling cases. And I hope that the Commission, which is now investigating gambling, will recommend that gambling be legalized. Because I cannot see the difference between the kind of gambling that we have sanctioned, like the OTB's, and the kind of gambling that is now outlawed.

And I really don't like to think of such a hypothetical question because it depends on the circumstances.

CHAIRMAN ERICKSON: Well, that is a moral question, so we will get out of the moral question and let's say it is narcotics. Well, I guess you could view the narcotics in the same light.

But if you will accept narcotics, supposing it is heroin that you are investigating and you have been told about this massive ring of heroin importers, and it turns out to be the sale of a lid of marijuana between two college students or just a restricted sale of a lid of marijuana.

When this comes up and is part of the progress report, should the judge dissolve the wiretap order?

PROFESSOR LAPIDUS: Mr. Chairman, I am afraid my answer will have to be the same on narcotics as on gambling, because I feel that wiretapping and all the electronic surveillance hasn't made one bit of difference in connection with the narcotics, either. I don't say I want to legalize narcotics, but I think we are approaching the problem in a very ineffective way.

We know that it is an international problem. We know that if we stop it at one point it comes in some other way. We used to get it from Marseilles,

now we get it from Mexico. We tackle it in a very ineffective way. And I hate to think of what that poor judge would have to do. I think the judge has a real problem there. And I would say if I had my way I would not use wiretapping or electronic surveillance to deal either with gambling or narcotics. I would limit it to murder, kidnaping, extortion where there is violence threatened—that sort of thing perhaps.

CHAIRMAN ERICKSON: All right. Let's put it on the extortion level.

What I am trying to get at is: Instead of having a crime of the scope outlined in the initial application, it turns out to be the most limited of crimes. Say it is an extortion crime that is alleged to involve organized crime and there is no indication of organized crime and there is only one threat when it was alleged to be widespread. What is the judge supposed to do? Dissolve the order and suppress that because it didn't meet the first application and didn't obtain the information they sought?

What is the judge supposed to do at that point?

PROFESSOR LAPIDUS: Are you asking me what he could do after the first report at the five-day point?

CHAIRMAN ERICKSON: Yes.

PROFESSOR LAPIDUS: No, as I said before, if you have 15 days you should be given the 15 days. But if you report to the judge that this is what you have after five days, well at least you have to show him that you still believe that it is a big operation, that even though this is all it is so far, you think there is more involved.

CHAIRMAN ERICKSON: The police officer very candidly says, "I was mistaken. This wasn't a big operation. All I got was this one isolated instance."

What does the judge do at that point?

PROFESSOR LAPIDUS: Well, I think that any law enforcement official who is worth his salt will terminate it of his own accord. If he admits he is mistaken, he will say, "Well, that is the end of the tap."

And there are many law enforcement officials who ask for 30 days and terminate it in less than 30 days. It doesn't happen often, that is true, but it does happen.

CHAIRMAN ERICKSON: All right. So he terminates the tap.

What happens to the elements he seized that didn't comply with the initial order?

PROFESSOR LAPIDUS: Well—

CHAIRMAN ERICKSON: All right, let's go further on this hypothetical.

Supposing that instead of the extortion that they thought they had, they come up with the sale of one

lid of marijuana. Should the police be able to prosecute that when they have obtained information which they weren't even seeking?

PROFESSOR LAPIDUS: Well, now of course, you get into problems there. You would have to get a court order. If you find that there is commission of some other offense, you simply can't use that evidence. You must get a court order to cover it. You can use it but you will have to do something further to comply with the law or it will be wasted.

But the law enforcement official would have to decide for himself whether it is serious enough for him to apply for a supplementary order and he may decide that he should do it or that he shouldn't.

CHAIRMAN ERICKSON: I understand that if they are going to conduct further surveillance on him they would have to do that.

PROFESSOR LAPIDUS: Yes.

CHAIRMAN ERICKSON: But what about the material they already have? Does the statute provide what should be done with the information that was obtained that doesn't fall within the four corners of either the application or what they were really looking for?

In short, does the fish that they found in the pond when they didn't think the fish was in the pond still get to be used?

PROFESSOR LAPIDUS: Well, now I am not clear about that. You know, this is a matter of evidence in criminal law and I am not a criminal lawyer. So I just—I wouldn't like to say yes or no, because it is a problem that I don't feel equipped to give a good answer on, or an answer that I would want the Commission to rely on.

CHAIRMAN ERICKSON: Do you feel that the requirements that are outlined in Title III for Federal use of electronic surveillance investigation are necessary, going all the way up to the Attorney General or his designated assistant?

PROFESSOR LAPIDUS: I cover the question of need, necessity, very fully in my book, *Eavesdropping on Trial*, and I have come to the conclusion that nobody has ever been able to prove need and nobody has ever been able to prove lack of need. So I don't think we can say yes and no, it is necessary or it isn't necessary. What we have to do is to balance the right of privacy against the needs of law enforcement.

CHAIRMAN ERICKSON: That is what I am asking you to do. I am asking you to give us your considered opinion as an expert as to whether or not the restrictions and the procedural safeguards that have been built into the Act are necessary or whether this could be simplified, for example, so that the United States Attorney at a local level could authorize this tap.

PROFESSOR LAPIDUS: Well, I would certainly be opposed to that.

CHAIRMAN ERICKSON: If you would object to that, then are you saying that someone other than the Attorney General or the Assistant that is designated by him should be authorized to do this? Should you have a specialist in the Attorney General's office who would do nothing but review wiretap applications so that he would be available 24 hours a day to act upon these applications?

PROFESSOR LAPIDUS: No, I can't say that I would feel that that would be an improvement. I think that the law as it now stands requiring approval of the Attorney General or of an Assistant Attorney General specially designated by him, is much better than doing it some other way.

The problem has been, as you know, in the past that orders have gone through, applications have been made, without the approval of the Attorney General.

CHAIRMAN ERICKSON: You are referring to the *Giordano* case. You are highlighting the *Giordano* case.

PROFESSOR LAPIDUS: Yes.

CHAIRMAN ERICKSON: Going to the state level, where would you draw the line? Should the attorney general of the states be the one that authorizes the tap on a local basis? Or should it be a local District Attorney, or should it be some other person?

PROFESSOR LAPIDUS: Now, that, too, is a state-by-state problem.

CHAIRMAN ERICKSON: That is right, and we are supposed to give an opinion. And we want your considered judgment on it.

PROFESSOR LAPIDUS: I wish I could help the Commission there. I wish I knew more about the set-up of the system of justice in all the states.

It is easy enough where it is a state like Georgia where they have an attorney general and he has this kind of function. Then you say, "Well, nobody but that attorney general can authorize it."

But in New York we do have a problem. Who is the one responsible for law enforcement? It should be somebody at the top level, and it should be impressed on the states that it can't be left to so many people.

One of the things that I did when I went around on interviews was to ask, "Who initiates these wiretaps? Who draws those papers? Who passes on them? Who authorizes them?"

And I was amazed at how many people had authority to initiate, to draw the papers—and some of those that I saw were pretty bad—and to follow through on the applications. And I know enough about the system—

CHAIRMAN ERICKSON: How would you improve that?

PROFESSOR LAPIDUS: I don't know how I would improve it. I know it needs improving but if the Commission went around and found out how these offices were set up it might find there is some supervision. Who does supervise these attorneys? Somebody has to be doing it. I don't know who.

CHAIRMAN ERICKSON: We will take a five-minute recess at this time.

[Whereupon a short recess was taken.]

CHAIRMAN ERICKSON: Professor Lapidus, I only have a few more questions, so may we continue?

We are filing your answers to the interrogatories as part of the record.

CHAIRMAN ERICKSON: One of the problems that goes to the heart of this question of requiring prior court authorization for the use of a consensual monitoring or recording device is that very often the police have an individual that isn't the confidential, reliable informant that is so often spoken of, but is one that is unreliable, and as a result he wouldn't be able to provide the probable cause but he has the information that shows a crime is being or is about to be perpetrated.

Now, should this use of a consensual eavesdropping device be limited to probable cause under *Spinelli* and *Aguilar*, or should there be a lesser test?

PROFESSOR LAPIDUS: I would say that we have to stay with probable cause, that it would really negate the purpose of requiring a court order if we do less, because the minute we get down to the reasonable suspicion rule, then we are dealing with something very unreliable.

No, I would say that if a law enforcement officer goes to a judge and says, "We need a court order for this," that he would have to show probable cause.

It might be that something less would satisfy the judge, and he would say, "Well, that is enough probable cause."

But I don't think that in the law you ought to say that anything less than ordinary probable cause would do. You know "probable cause" is a very elastic term. It has been defined but it is being constantly litigated as to whether or not there was probable cause.

CHAIRMAN ERICKSON: Certainly it has been litigated, but if there is that elastic, there is no reason for requiring it, is there?

PROFESSOR LAPIDUS: No, I wouldn't say that. The mere fact that there is a little give and take that way doesn't mean that you shouldn't require it.

No, I would not like to accept the view that—

CHAIRMAN ERICKSON: Reasonable suspicion?

PROFESSOR LAPIDUS: No, I don't think so. As I said before, it is this one problem of consensual eavesdropping that seems to be troubling the Commission to which I haven't really given that much thought, so I am not sure that I can be very helpful.

CHAIRMAN ERICKSON: Well, I will only say that the thought that you put forth in preparing the answers to the interrogatories shows your depth of knowledge on the subject, and we are indeed delighted that you were able to give us the time to prepare those answers and to file these reports that you have made available to the Commission that will assist us so much in our deliberations.

Professor Blakey.

PROFESSOR BLAKEY: I have no questions, but I would like to extend to Professor Lapidus my thanks for coming. I have read your book, as you know, and I have studied very carefully your suggestions, both in the book and in the materials you prepared for us, and I am certainly very appreciative of your ability to stay over today.

Thank you very much.

PROFESSOR LAPIDUS: Thank you, Mr. Chairman and members of the Commission. I enjoyed listening all day long yesterday. I listened very carefully, and I think I learned a great deal from the discussion and I certainly came away with the feeling that the Commission was doing a very careful job of investigating both the law and the practice on wiretapping electronic surveillance.

And I leave Washington with a very good feeling that the whole problem—and it is a very serious problem—is in good hands.

CHAIRMAN ERICKSON: We are very grateful to you, and thank you very much for staying with us. We know the inconvenience that your stay has caused you and we are doubly appreciative for that reason.

[The prepared statement of Edith J. Lapidus follows.]

STATEMENT OF EDITH J. LAPIDUS,
PROFESSOR, QUEENS COLLEGE,
CITY UNIVERSITY OF NEW YORK

Mr. Chairman and Members of the Commission: I appreciate the opportunity of appearing before you today to discuss the problems involved in Federal and State laws and practice relating to wiretapping and electronic surveillance. This Statement is addressed to the specific questions outlined in the Commission's Questionnaire dealing with court-ordered electronic surveillance. It supplements my answers submitted to the Commission on May 14, 1975.

In April 1974 I presented a Statement on Wiretapping and Electronic Surveillance under Title III to the Subcommittee on Courts, Civil Liberties, and the Administration of Justice, of the House Committee on the Judiciary. The Statement appears on pages 259-274 of the Hearings of the Subcommittee held April

24, 26, and 29, 1974 (Serial No. 41). In that Statement, as in my book *Eavesdropping on Trial* I tried to be as objective, unbiased, and impartial as possible, and to offer some constructive and realistic proposals for changes in law and practice. Some changes that seemed unlikely to meet with approval by Congress or the public a year ago now appear possible. This Statement will emphasize proposals that may restore some of the privacy invaded by government electronic surveillance without unduly interfering with law enforcement.

Question 2.

Is court-ordered eavesdropping necessary for investigation of criminal conspiracies or organized criminal activity? Is it necessary in investigating narcotics and gambling rings? Would use of informants or undercover agents be preferable?

As to whether it is "necessary": A decade of hearings in Congress produced nothing but conflicting expert opinion on the question of need for wiretapping and electronic surveillance. No one ever succeeded in proving need, or even in defining it clearly. Nor was it ever settled who should bear the burden of proving need. If the Commission is to determine whether court-ordered eavesdropping is necessary, it will have to compare time and cost factors. Would the same resources devoted to normal types of surveillance produce equal or better results, or no results at all? If Title III has not been used effectively against organized crime or limited to serious offenses, the need for court-ordered eavesdropping to promote public safety is seriously weakened in balancing it against the invasion of privacy that it necessarily entails.

What is "organized crime" or "organized criminal activity"? Title III was intended to deal primarily with organized crime. This was the reason offered most frequently for passage of the law and Congress acknowledged this need in its introductory findings. However, it did not define "organized crime." It is doubtful that the intent to reach "organized crime" has been carried out. Law enforcement officials admit freely that they go after the most important suspected criminal figures that they can reach. Top echelon members are carefully shielded. There is nothing in the reports required by Title III to indicate the level of organized crime covered by a court order, or whether organized crime is involved.

The vast majority of orders obtained under Title III have related to gambling and narcotics (about 80% in 1974). Recommendations have been and are still being made to legalize gambling and to treat narcotics as an illness at the lower levels and as an international problem to stop the flow of drugs into the United States. If gambling and narcotics were removed from ordinary law enforcement, applications for court orders would dwindle to a negligible number.

A tremendous amount of effort and huge sums have been devoted to dealing with gambling and narcotics—whether through court-ordered eavesdropping or the use of informants and undercover agents. Perhaps it is time to rethink our social policy on these problems. Court-ordered eavesdropping involves an intrusion on privacy. Use of informants or undercover agents often involves the government in actual, if not legal, entrapment. Which is preferable? I believe it is a poor choice either way.

Question 3.

Is the list of crimes for court-ordered surveillance adequate? Should it be more limited?

Section 2516(1) presents a long list of offenses for which Federal officers may seek a court order. They were selected, according to the Senate Report because they were characteristic of activities of organized crime or because of their seriousness. However, eavesdropping in any offense seems to be sanctioned on the theory that organized crime has not limited itself to the commission of any particular offense.

The list of offenses in which State officials may obtain a court order is shorter, but perhaps even broader than that of the Federal government [Section 2516(2)]. The State list appears to be practically unlimited. State statutes may authorize eavesdropping in connection with:

... the offense of murder, kidnapping, gambling, extortion, or dealing in narcotic drugs, marihuana, dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute ... or any conspiracy to commit any of the foregoing offenses.

There is great potential for abuse inherent in permitting wiretapping and electronic surveillance over a wide spectrum of offenses. The reports required by Title III do not reveal the seriousness of the offense or whether organized crime was involved. I believe that if court-ordered surveillance is to be continued, it should be restricted to serious crimes, in both Federal and state proceedings.

Question 4.

Should electronic surveillance upon consent of one party to the conversation be proscribed? Should there be an exception for law enforcement? Should it be subject to court order, regulation, or reporting?

Section 2511(2)(c) declares that it is not unlawful for a law enforcement officer to intercept a wire or oral communication if he is a party to the communication or if one of the parties gave prior consent to the interception. This provision was no innovation in policy. It reflected the decisions of the United States Supreme Court which, over a period of two decades, had generally sanctioned eavesdropping without a warrant if one of the parties to the conversation gave his consent to the interception.

Prior to enactment of Title III, the leading cases on the subject of consent eavesdropping were *On Lee v. United States*, 343 U.S. 747 (1953) and *Lopez v. United States*, 373 U.S. 427. *On Lee* involved third-party monitoring of conversations; *Lopez* rules on single-party informant "bugging." In *On Lee* the Supreme Court upheld the right to wire an informant for sound in order to transmit statements of a suspect to police officers listening at a receiver outside the building. In *Lopez*, a government agent was equipped with a pocket wire recorder which recorded conversations of a cabaret operator offering a bribe to an agent to help him conceal tax liability. The Supreme Court ruled that the evidence obtained through the recording device was admissible in evidence and that there was no violation of the Fourth Amendment to the Constitution, although no warrant had been obtained.

The traditional principle on which the validity of consent eavesdropping without a warrant rests is that a party to a conversation takes his chances that the other participant may increase his present or future audience. Justice Brennan, dissenting in *Lopez*, protested that "in a free society people ought not to have to watch their every word so carefully."

Since enactment of Title III, the Supreme Court has held that the Fourth Amendment is not violated by governmental electronic eavesdropping effected by wiring an informant for sound, having him talk to the suspect, and then having agents to whom the conversation is transmitted repeat the communications at the suspect's trial [*United States v. White*, 401 U.S. 745 (1971)]. Deep cleavages in the Supreme Court on the subject of consent eavesdropping were revealed by the opinions of the Justices in *White*. The Court reversed the judgment of the Court of Appeals and upheld White's conviction by a vote of 6 to 3, but no agreement could be reached on a majority opinion.

The plurality view in *White*, expressed by Justice White, had the support of Chief Justice Burger and Justices Stewart and Blackmun. Justice Brennan concurred in the result on the technical ground that *Katz v. United States* was not retroactive.

Justice Black concurred in the judgment because of his view that electronic surveillance is not a search and seizure subject to the Fourth Amendment. Dissenting opinions were filed by Justices Douglas, Harlan, and Marshall. The issue as Justice Harlan saw it in his dissenting opinion was whether "uncontrolled consensual surveillance in an electronic age is a tolerable technique of law enforcement, given the values and goals of our political system. Third-party bugging, he believed, undermined that confidence and sense of security in dealing with one another that is characteristic of individual relations in a free society. Justice Douglas based his dissent not only on the Fourth Amendment but also on freedom of speech guaranteed by the First Amendment. Must everyone live in fear that every word he speaks may be transmitted or recorded, he asked. He could imagine nothing that has a more chilling effect on people expressing their views on important matters.

Several bills have been introduced in Congress to eliminate the exception of "consent eavesdropping" from court order requirements of Title III, and to permit a person to record electronically or otherwise intercept a wire or oral communication only where *all* the parties to the communication have given prior consent to such interception. This is an ideal solution to a troublesome problem. In my Statement a year ago to the Subcommittee on Courts, Civil Liberties, and the Administration of Justice, of the House Committee on the Judiciary, I expressed doubt that Congress and the public would support outlawing one-party-consent eavesdropping. I believe that the climate of opinion has changed.

Unless all the parties to a conversation consent, the recording of such conversations should be proscribed unless a prior court order is obtained, and reports on such orders should be made to the Administrative Office of the United States Courts.

Question 5.

Is responsibility for authorization of application for court ordered electronic surveillance properly placed? Is the Federal system too centralized? Is the State system too decentralized?

It seems proper to limit power to authorize applications to the Attorney General, or any Assistant Attorney General specially designated by the Attorney General. The difficulty in the past has been that the Attorney General did *not* personally authorize each application. As to the States, it would seem that too many people can apply for orders. Authority is given to "the principal prosecuting attorney" of the State or *political subdivision*. In Georgia, applications are made by one individual, the State Attorney General, but in New York dozens of persons may and do submit requests for orders. New York State has 62 counties, each with its own District Attorney. Any one of these may apply for a court order, and there is no supervision of his actions other than by the judge who issues the order. In many cases, the judges to whom applications are presented were former District Attorneys. Judges who prior to their ascent to the bench were attorneys representing defendants in criminal cases are not very sympathetic to applications for court orders for wiretapping or electronic surveillance. It is possible to go "judge-shopping."

Perhaps some means could be devised for supervision of District Attorneys who apply for court orders. Perhaps training programs sponsored by the Law Enforcement Assistance Administration could impress them with the fact that court-ordered electronic surveillance is a serious intrusion on privacy and should be used only in the case of serious offenses.

Question 6.

Is there a role for greater judicial supervision? Should progress reports be required? Should emergency interceptions be subject to prior judicial approval?

Section 2518(6) provides that an order *may* require periodic reports to the judge showing what progress has been made and

the necessity for continued interception. Progress reports are intended to serve as a check on the continuing need to conduct the surveillance and to prevent abuse. Federal judges are reported generally to require progress reports. Few, if any State judges have specified in the court order that progress reports shall be submitted, although some say that they receive oral progress reports from time to time. This may seriously undermine judicial supervision of the operator who is listening to intercepted conversations and of the law enforcement official who is handling the investigation.

Progress reports to judges should be *mandatory* and not discretionary. Failure to require such reports is an obvious gap in judicial supervision, and should be remedied.

Sec. 2518(7) of Title III permits wiretapping and electronic surveillance by government officials without court order during a 48-hour emergency. Emergency situations are described as involving two types of conspiratorial activity: (1) threatening national security, and (2) characteristic of organized crime. I believe that the emergency clause is vague, open to abuse, and unconstitutional. National security is not defined, and the law does not indicate what offenses are 'characteristic of organized crime.' No report is required to be filed, and there is no way of knowing how much 'emergency' eavesdropping has been going on. The law requires that all conditions necessary for issuance of an order under Title III be present before emergency surveillance begins, but it is unrealistic to assume that these conditions will always be satisfied.

Federal officials have claimed that the 48-hour emergency provisions have never been utilized. On the State level, New Jersey appears to be the only one to have provided for emergency eavesdropping. The New Jersey law is more restrictive than Title III. Informal application may be made to a judge who may grant verbal approval without an order, to be followed within 48 hours by application for an order. It must relate to investigation of conspiratorial activities of organized crime. If no application is made, or if the application is denied, the taped recordings of conversations must be delivered to the court and sealed. Failure to do so is punishable as contempt of court. The District of Columbia law also provides for emergency eavesdropping; application for an order must be initiated within 12 hours of the emergency and be completed within 72 hours.

In the debate in Congress to restrict an emergency situation to one involving imminent threat to human life, Senator Philip A. Hart (D. of Mich.) commented on the vagueness of the word "emergency:"

If one is a good policeman everything is an emergency to him. I believe that the 48-hour emergency provision is an invitation to misuse and opens up possibilities for "leads" and corroborative information rather than obtaining specific evidence of a particular crime. It should be repealed. In an emergency, a court order can always be obtained without delay.

Question 7.

Is the 30-day period for a wiretap or 'bug' too lengthy? What would be adequate? Should the number of extensions be limited? Is provision permitting postponement of notice necessary?

Many State court orders have provided for interception during the maximum thirty-day period, and renewals have been granted freely. This period is too long, and Sec. 2518(5) allowing interception for a period up to 30 days with an unlimited number of 30-day extensions should be amended.

Federal orders have generally limited the period to 15 days and this seems like a reasonable maximum length of time. Requests for orders covering a longer period than is necessary frustrate the specific requirements of the law.

As to extensions, these should be limited. State and Federal officials claim that an extended period is needed where the offense is a continuing one, but some admitted frankly that extensions were sometimes asked in order to postpone giving notice of the interceptions. The granting of an unlimited number of exten-

sions also gives rise to the suspicion that a law enforcement official may be engaging in "strategic intelligence" surveillance, instead of attempting to obtain specific evidence of a specific crime. An extension for a maximum of 10 days could be the rule, with some leeway in unusual circumstances.

The power of a judge to postpone giving notice should be limited specifically where the individual whose communication is intercepted is not engaged in a continuing criminal enterprise. In cases where postponement is permitted because of a continuing criminal enterprise, the judge and prosecuting official should be required to issue a detailed report when notice is finally given.

Question 8.

Should standards for minimization of electronic surveillance interceptions be set forth in Title III? What standards?

One way of minimizing interception of innocent conversations is to ban automatic monitoring and to require manual or 'live' monitoring. In live monitoring, police officers or agents sit continuously at the receiving station, listening to the recordings and making notes of relevant conversations. The recorder can be shut off when innocent, irrelevant, or privileged conversations are taking place—if they can be recognized as such. In automatic recording, the conversations are recorded on tapes without listeners and are later played back at intervals, the frequency depending on the circumstances and on the practice established in a particular office. The automatic device records all conversations.

The law is not clear as to whether automatic recording is prohibited, and it is done at least in some State law enforcement agencies.

Even if live monitoring is used, administrative regulations are needed to control the agents who man the monitoring devices. Recommendations of the American Bar Association made in 1971 are as follows:

1. Limit the number of agents authorized to employ the techniques.
2. Specify the circumstances under which the techniques may be used, giving preference to those which invade privacy least.
3. Set out the manner in which techniques must be used to assure authenticity.
4. Provide for close supervision of agents.
5. Circumscribe acquisition and custody of, and access to electronic equipment by agents.
6. Restrict transcription, custody of, and access to overheard or recorded communications by agents.
7. Provide training programs for agents.

Following items 4, 5, and 7 would do much to minimize interceptions.

It should also be made clear that the gathering of strategic intelligence is not permitted by Title III. An application for a court order must show that a *particular offense* has been, is being, or is about to be committed [Sec. 2518(1)(b)(i)]. This would seem to limit applications to those seeking specific information about a particular crime—that is, tactical, as distinguished from strategic intelligence.

Question 9.

Should distinctions be made in the law between wiretapping and "bugging"? Should an applicant be required to specify if breaking and entering is required and obtain specific authorization?

I do not see any need to distinguish between wiretapping and "bugging". Wiretapping is the interception of telephone calls and normally involves a physical entry into a telephone circuit. "Bugging" is listening in on conversations in a given area by means of electronic devices. It is sometimes hard to tell where wiretapping leaves off and electronic surveillance begins. All telephones have wires and some miniature listening devices do

too. In both, the intercepted conversations are recorded on tape. The technique of one is sometimes affected by the other. Most of the court orders under Title III have been obtained for *wiretapping* and breaking and entry have not been necessary. If an order covers electronic surveillance involving breaking and entering, it would be well to require that the order explicitly authorize it.

Question 10.

Is privacy best protected by storage under seal of tapes for a 10-year period? Should information be preserved permanently? Could tapes be destroyed sooner than in 10 years, on notice and hearing?

I can see no objection to the requirement of Sec. 2518(8)(a) that recordings shall not be destroyed except on order of the issuing judge and in any event shall be kept for ten years. A problem may arise, however, as to HOW they are sealed, a matter that is not covered by Title III. In the case of documents—the application, affidavits, order, etc., the common practice is simply to put the papers in a folder, bind it with adhesive tape, and have the judge put his signature across the tape. The seals are rather makeshift affairs and tampering should not be too difficult.

Question 11.

Are reports to the Administrative Office necessary? What additional facts should be reported? Should illegal taps be reported?

The reports to the Administrative Office do serve a useful purpose. At the least, they act as a deterrent to requests for too many orders by prosecuting officials, and to acquiescence by judges. The information is collated by the Administrative Office of the United States Courts and Congress will know who asked for the orders and who granted them. The difficulty is that neither judges nor prosecuting officials take the reports seriously. Some judges think it is a nuisance and shift the task to the prosecuting official. All the judge does is sign his name. Law enforcement officials also find the reports a source of irritation; State officials have complained that the following items of the report are vague and objectionable:

1. Average frequency of intercept.
2. Number of persons whose communications were intercepted.
3. Number of communications intercepted.
4. Number of incriminating communications intercepted.
5. Number of convictions.
6. Cost.

Instead of requiring average frequency of intercept, the report should require a statement of the total number of days in which interception actually occurred out of the total number of days authorized. Number of communications intercepted should be clarified to include attempted as well as completed calls, for numbers calling or called can serve to identify persons connected with the suspect. Number of incriminating communications intercepted is ambiguous, since it is not clear when a conversation is "incriminating." The number of convictions may be misleading. Officials should be required to indicate whether the conversations intercepted were used as evidence in obtaining a conviction, and whether in their opinion these intercepted communications contributed substantially to conviction and whether evidence was obtained by other investigative techniques and used.

Cost should include a statement of the exact amount paid to each investigator and all other individuals who spent time on the particular wiretap. It should be made clear that it includes cost of equipment, plant, and any other items of expense involved in interception of conversations, recording, and making logs and transcripts.

Question 12.

Is Title III effective in prohibiting manufacture, distribution, possession, advertising of interception devices? Should manufacturers be licensed? How can proliferation of equipment be stemmed? Should the FBI investigate illegal wiretapping by local police?

The ban on private eavesdropping in Title III is completely ineffective. The prohibition against manufacture, distribution etc. applies only to devices designed *primarily* for *surreptitious* wiretapping and electronic surveillance. Suppliers claim they sell only to law enforcement officials. But a private individual does not have to go to a manufacturer or distributor in the business. He can buy parts at an electronics supply house and put them together with a little electronics experience. It is estimated that there are 200,000 people in the United States who know how to assemble an electronic eavesdropping device. Since that estimate was made, the number of young experts has probably increased. Licensing of manufacturers would be futile. The only way to stem proliferation of equipment is to enforce the law vigorously. Officials must wait for complaints, and State officials say that few complaints have been received. The U.S. Department of Justice has had some complaints, but few prosecutions have resulted.

The F.B.I. hardly qualifies as the agency to investigate illegal wiretapping. Perhaps we should go back to the Right of Privacy Act of 1967 and ban ALL wiretapping and electronic surveillance except in national security cases. That would surely stem proliferation of electronic listening devices.

Question 13.

Is exception to communications common carriers too broad? Should the law proscribe interception of telephone communications of employees by employers? How about those who conduct most of their business by telephone? Does an employee have an expectation of privacy on a business telephone?

Section 2511(2)(a) exempts from the prohibition against interception employees or agents of "communications common carriers" in the normal course of employment, but such carriers are forbidden to use service observing or random monitoring except for service quality control checks. This seems to be a reasonable provision. Its effectiveness depends on the vigilance and good faith of the telephone company.

I do not believe that there is any expectation of privacy in communications by an employee on a business telephone, nor should the law grant such privacy specifically

SUMMARY

I believe that prosecuting officials, judges, and others involved in law enforcement want to comply with the law relating to wiretapping and electronic surveillance and with the Constitution. They are looking for guidance, for clarification of ambiguities in the law, and for correction of defects in practice. By its recommendations the National Commission can furnish that guidance. I urge the Commission to propose that Congress make the following changes in Title III of the Omnibus Crime Control and Safe Streets Act of 1968:

1. Limit covered offenses to serious crime.
2. Make progress reports to judges mandatory.
3. Ban interceptions without court order unless all parties to a conversation consent.
4. Reduce the initial period of interception to a maximum of 15 days, with one extension of 10 days, except in unusual circumstances.
5. Eliminate the 48-hour emergency exception to court order requirements.
6. Prohibit automatic monitoring of conversations and require manual or live monitoring of interceptions.

7. Clarify the fact that a court order is obtainable only to obtain specific evidence of a specific crime, and not to gather strategic intelligence.

8. Require an applicant for an order to specify if breaking and entering is required and obtain specific authorization for such intrusion.

Law enforcement officials need not wait for Congress to act. They can limit applications to serious crime, make progress reports, ask for 15-day orders instead of 30. They can minimize interceptions by using live monitoring exclusively, and refrain from attempting to gather strategic intelligence. The Commission should urge that they do so. The following additional changes in practice should also be recommended:

1. Provide for closer supervision of monitoring agents.
2. Institute training programs for prosecuting officials so that they understand the safeguards provided by law.
3. Make certain that seals are secure so that tampering is difficult or impossible.
4. Clarify details of the reports to the Administrative Office of the United States Courts.

I believe that if these changes in law and practice are made, some of the privacy that has been lost in sanctioning and encouraging wiretapping and electronic surveillance will be restored without any undue interference with law enforcement to combat crime.

Statement of Professor Edith J. Lapidus on Wiretapping and Electronic Surveillance, under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice, of the House Committee on the Judiciary, on Monday, April 29, 1974 at 10 A.M.

TABLE OF CONTENTS

Purposes and Provisions of Title III

- Court-ordered eavesdropping
- Eavesdropping without court order
- Consent eavesdropping

Defects in court-ordered eavesdropping

- Offenses covered
- Specific offense or strategic intelligence
- The particularity requirement
- Judge-shopping for court orders
- Overhearing innocent or privileged conversations
- Time period for interception of conversations
- Notice of eavesdropping, objections, and disclosures
- Reports on court-ordered eavesdropping

Evaluation of Eavesdropping under Title III

- Minimizing invasion of privacy
- The need for eavesdropping
- Effectiveness of eavesdropping under Title III

Summary of Proposals

United States Supreme Court Decisions

Mr. Chairman, members of the Committee: My name is Edith J. Lapidus. I am a member of the New York Bar and am admitted to practice before the United States Supreme Court. I teach Constitutional Law at Queens College of the City University of New York and hold a Ph.D. degree in Political Science from the City University. My book, *Eavesdropping on Trial*, with a Foreword by Senator Sam J. Ervin Jr., was released by Hayden Book Company Inc. of Rochelle Park, New Jersey, in January 1974. It presents an analysis and evaluation of the law and prac-

tice under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 in which Congress, for the first time in the history of the United States, sanctioned wiretapping and electronic surveillance by government officials.

I deeply appreciate this opportunity to appear before you and to discuss the problems associated with government eavesdropping and the conflict that it raises between the individual's right to privacy and society's need for effective law enforcement in dealing with crime. This complex and controversial subject has suffered in the past from ideological and political partisanship, and (at least before "Watergate") from public indifference. In my study of wiretapping and electronic surveillance under Title III of the 1968 Act, I have tried to be as objective, unbiased, and impartial as possible, and to offer some constructive and realistic proposals.

This Statement is based largely on my findings as reported in *Eavesdropping on Trial*, but it also includes proposals suggested by events that have occurred since the book went to press and further reflection. Problems of *court-ordered* wiretapping and electronic surveillance by law enforcement officials are emphasized in this Statement and discussed in detail. Criticism of *warrantless* eavesdropping, a serious loophole in Title III considered fully in my book, is merely outlined here.

PURPOSES AND PROVISIONS OF TITLE III

Title III is one of eleven "Titles" in the Omnibus Crime Control and Safe Streets Act of 1968, passed by Congress in the wake of a nationwide fear of crime and clamor for "law and order." It purports to serve a dual function:

1. To protect the privacy of individuals by banning *private* eavesdropping, and prohibiting manufacture, sale, possession, or advertising of eavesdropping devices designed primarily for surreptitious interception.

2. To combat organized crime and other serious offenses by giving law enforcement officials an effective tool—interception of wire and oral communications, under specified conditions and with proper safeguards.

The 1968 law is an attempt to balance "liberty" against "law and order." It prohibits interception of wire and oral communications and then makes certain exceptions: designated Federal and State officials are authorized to intercept such communications in the case of specified offenses, provided they comply with procedures detailed in the law. The heart of this procedure is the obtaining of a *court order* from a judge of designated courts, similar to a warrant for search and seizure. In some instances, eavesdropping by law enforcement officials is permitted *without* court order.

Court-ordered Eavesdropping

The safeguards to individual privacy sought to be provided by Title III consist of requiring a court order before a government official may intercept a wire or oral communication. A judge is to decide whether or not an order shall be issued, and the interception is subject to supervision by him. Title III lists a wide variety of offenses for which a court order may be obtained, the Federal officers who may apply for a court order, the judges to whom applications must be presented, and the necessary findings by the judge of "probable cause" on which orders are to be based. State officials may also apply for court orders to wiretap or conduct electronic surveillance provided the particular State enacts a law conforming to Title III.

An order may be granted for a period not exceeding thirty days, with an indefinite number of renewals, each for a period up to thirty days. Notice of the interception must be given to the persons named in the order or application, and to others in the discretion of the judge, within ninety days after termination. Judges and prosecuting officials are required to file reports on each order with the Administrative Office of the United States

Courts in Washington, D.C., and this agency, in turn, must file an annual report with Congress.

Heavy penalties are provided for violations of Title III: imprisonment up to five years and a fine of \$10,000 or both. Civil damages are also recoverable—actual damages but not less than liquidated damages computed at the rate of \$100 a day for each day of violation, or \$1,000, whichever is higher; punitive damages and counsel fees and other litigation costs are also recoverable. Conversations intercepted unlawfully are barred from introduction in evidence.

These seemingly simple provisions for court-ordered eavesdropping by government officials have raised some difficult legal and practical questions and generated much heated discussion. They purport to comply with requirements of the United States Supreme Court laid down in two landmark decisions handed down in 1967, *Berger v. New York* (388 U.S. 41) and *Katz v. United States* (389 U.S. 347), and law enforcement officials claim that their practices follow the mandates of the Supreme Court. *Berger* struck down as unconstitutional a New York law permitting court-ordered eavesdropping on the ground that the statute was "too broad in its sweep" and failed to provide adequate judicial supervision or protective procedures. In *Katz*, the Supreme Court held for the first time that electronic surveillance constitutes a "search and seizure" subject to the protections and limitations of the Fourth Amendment to the United States Constitution which provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Critics of Title III protest that the safeguards sought to be provided by the court order requirements are inadequate; that many terms and clauses in the law are ambiguous; that State and Federal officials are misinterpreting some provisions and failing to carry out others. My study of the law and practice under Title III has led me to the conclusion that there is validity in these criticisms, and I shall discuss them in detail later in this Statement. Even the most ardent proponents of government eavesdropping will admit, I think, that no acceptable balance between "liberty" and "law and order" can be achieved without clarity in the law, existence and observance by law enforcement officials of proper standards and guidelines, and scrupulous adherence to the safeguards sought to be provided by Title III.

Eavesdropping Without Court Order

In addition to court-ordered eavesdropping, the Federal law permits wiretapping and electronic surveillance by government officials *without* court order in two broad types of cases: (1) during a forty-eight-hour emergency, and (2) to protect "national security" under authority of the President. *Emergency* situations are described as involving two types of conspiratorial activity:

1. threatening national security, and
2. characteristic of organized crime.

The emergency clause [Sec. 2518 (7)] has been widely attacked as vague, open to abuse, and unconstitutional. The term "national security" is not defined, and the law does not indicate what offenses are "characteristic of organized crime." No report is required to be filed, and there is no way of knowing how much "emergency" eavesdropping has been going on. The law requires that all conditions necessary for issuance of an order under Title III be present before emergency surveillance begins, but it seems unrealistic to assume that these conditions will always be satisfied. The conclusion is compelling that if emergency eavesdropping without court order should be permitted at all, it should be restricted to cases involving a threat to actual or potential attack by a foreign power, collection of foreign intelligence information, or investigation of espionage activity.

In addition to the emergency clause, exemption from court order requirements is provided for national security related eavesdropping undertaken "by authority of the President" [Sec. 2511 (3)]. Title III declares that nothing in the Act shall limit the constitutional power of the President to take measures that he deems necessary:

1. To protect the Nation against actual or potential attack or other hostile acts of a foreign power;
2. To obtain foreign intelligence information deemed essential to the security of the United States; or
3. To protect national security information against foreign intelligence activities.

Nor is any limitation to be placed on the constitutional power of the President to protect the United States against: (1) overthrow of the Government by force or other unlawful means, or (2) any other clear and present danger to the structure or existence of the Government. Interception without court order must, however, be "reasonable," if the communications are to be received in evidence in any trial, hearing, or other proceeding.

Warrantless eavesdropping under presidential authority has raised a storm of protest that has not yet fully subsided. Many who were willing to accept court-ordered eavesdropping to combat crime denounced the provision dispensing with judicial sanction as highly ambiguous and unconstitutional. Objections increased in bitterness when the Government claimed that national security may involve threats from *domestic* groups as well as from foreign powers, and it was revealed that Federal agencies had tapped the telephones of political dissidents without court order. On June 19, 1972, the United States Supreme Court ruled, by a vote of 8 to 0, that presidential authority to protect the nation does not give the Government power to tap without court order the wires of domestic radicals who have "no significant connection with a foreign power, its agents, or agencies" (*United States v. District Court*, 407 U.S. 297).

The opinion in the case against the District Court was written by Justice Powell. While the decision was hailed as a victory by civil libertarians, the objections to warrantless eavesdropping in national security cases have by no means subsided, nor are the problems fully resolved. The Government may still claim that some radicals whose phones have been tapped without court order do have "a significant connection with a foreign power, its agents, or agencies," thus removing them from Fourth Amendment protection. The decision of the Supreme Court may also have left a loophole by suggesting that traditional warrant requirements were not "necessarily applicable" in domestic security cases.

United States v. District Court is a first step in outlawing government eavesdropping without court order in domestic security cases. Warrantless interception circumvents the "probable cause" requirement; and no disclosure to a judge or anyone else need ever be made. There is no way for Congress or the public to know how much eavesdropping is going on if no court order is obtained. "Domestic security" is a vague concept, and it may be difficult to determine if a threat is foreign or domestic without first tapping or bugging. If adequate delineation is impossible, then the warrant procedure should be required in all cases and no "national security" exception to a court order should exist. For a detailed discussion of warrantless eavesdropping in so-called national security cases, see *Eavesdropping on Trial*, page 96 et seq. Since publication of the book, I have come to the conclusion that Congress must make it impossible to engage in illegal eavesdropping under the shield of "national security" by requiring a court order in this type of investigation. H.R. 9781 introduced by Mr. Kastenmeier on March 28, 1974 in the House of Representatives appears to effect such a change in Title III by defining a "foreign agent" and requiring a court order in national security cases.

Consent Eavesdropping

One of the exceptions from court order requirements of Title III is "consent" eavesdropping. Section 2511(2)(c) declares that it is not unlawful for a law enforcement officer to intercept a wire or oral communication if he is a party to the communication or if one of the parties gave prior consent to the interception. This provision of the law was no innovation in policy. It reflected the decisions of the United States Supreme Court which, over a period of two decades, had generally sanctioned eavesdropping without a warrant if one of the parties to the conversation gave his consent to the interception.

Prior to enactment of Title III the leading cases on the subject of consent eavesdropping were *On Lee v. United States*, 343 U.S. 747 (1953) and *Lopez v. United States*, 373 U.S. 427 (1963). *On Lee* involved third-party monitoring of conversations; *Lopez* ruled on single-party informant "bugging." In *On Lee*, the Supreme Court upheld the right to wire an informant for sound in order to transmit statements of a suspect to police officers listening at a receiver outside the building. In *Lopez*, a government agent was equipped with a pocket wire recorder which recorded conversations of a cabaret operator offering a bribe to an agent to help him conceal tax liability. The Supreme Court ruled that the evidence obtained through the recording device was admissible in evidence and that there was no violation of the Fourth Amendment to the Constitution, although no warrant had been obtained.

The traditional principle on which the validity of consent eavesdropping without a warrant rests is that a party to a conversation takes his chances that the other participant may increase his present or future audience. Justice Brennan, dissenting in *Lopez*, protested that "in a free society people ought not to have to watch their every word so carefully."

Since enactment of Title III, the Supreme Court has held that the Fourth Amendment is not violated by governmental electronic eavesdropping effected by wiring an informant for sound, having him talk to the suspect, and then having agents to whom the conversation is transmitted repeat the communications at the suspect's trial [*United States v. White*, 401 U.S. 745 (1971)]. Deep cleavages in the Supreme Court on the subject of consent eavesdropping were revealed by the opinions of the Justices in *White*. The Court reversed the judgment of the Court of Appeals and upheld *White's* conviction by a vote of 6 to 3, but no agreement could be reached on a majority opinion.

The plurality view in *White*, expressed by Justice White, had the support of Chief Justice Burger and Justices Stewart and Blackmun. Justice Brennan, who had dissented in *Lopez* concurred in the result, but only on the technical ground that *Katz v. United States* was not retroactive. Justice Black concurred in the judgment, but only because of his view that electronic surveillance is not a search and seizure subject to the Fourth Amendment. Dissenting opinions were filed by Justices Douglas, Harlan, and Marshall.

According to the plurality opinion, the question to be decided was this: what expectations of privacy are constitutionally "justifiable"—what expectations will the Fourth Amendment protect in the absence of a warrant? A police agent who conceals his identity may write down his conversations with a defendant and testify concerning them without a warrant. No different result, said the Court, is required if the agent records the conversations with electronic equipment carried on his person (as in *Lopez*) or carries radio equipment which transmits the conversations to recording equipment located elsewhere or to agents monitoring the transmitting frequency (as in *On Lee* and in *White*).

The three dissenters, Justices Harlan, Douglas, and Marshall, objected to equipping agents with eavesdropping devices in the absence of a court order, but approved of use of informants without judicial supervision. Some critics suggested that "a far greater danger to our free society is presented by the prospect

that friends and associates may be employed as government spies" than by equipping informants with electronic transmitting devices. The issue as Justice Harlan saw it in his dissenting opinion was whether "uncontrolled consensual surveillance in an electronic age is a tolerable technique of law enforcement, given the values and goals of our political system." He considered third-party monitoring a greater invasion of privacy than single-informant bugging. Third-party bugging, he believed, undermined that confidence and sense of security in dealing with one another that is characteristic of individual relations between individuals in a free society.

The dissent of Justice Douglas in *United States v. White* was much sharper than that of Justice Harlan. Justice Douglas could see no excuse for not seeking a warrant in the *White* case. He based his dissent not only on the Fourth Amendment ban on unreasonable search and seizure, but also on freedom of speech guaranteed by the First Amendment. Must everyone live in fear that every word he speaks may be transmitted or recorded, he asked. He could imagine nothing that has a more chilling effect on people expressing their views on important matters. (Consent eavesdropping and *White* are discussed more fully in *Eavesdropping On Trial*, p. 28 et seq.).

Several bills have been introduced in the House of Representatives to eliminate the exception of "consent eavesdropping" from court order requirements of Title III, and to permit a person to record electronically or otherwise intercept a wire or oral communication only where *all* parties to the communication have given prior consent to such interception (H. R. 9667; 9781; 9698; 9973; 10008; 10331). This is an ideal solution to a troublesome problem, but a proposal to outlaw warrantless consent eavesdropping will undoubtedly meet with fierce resistance by law enforcement officials and others. This type of electronic surveillance is reported to be used in tens of thousands of investigations each year. The practice is so firmly entrenched in law enforcement and the burden of dealing with crime is so great that public support for outlawing one-party-consent eavesdropping is far from certain. Businessmen and private individuals who routinely record telephone conversations can be expected to join in defending the practice.

Defects in Court-Ordered Eavesdropping

Seven problem areas of court-ordered eavesdropping have been identified that require attention by Congress or the courts and that must be solved if wiretapping and electronic surveillance by law enforcement officials is to be permitted to continue:

1. Offenses for which an order may be obtained are practically unlimited, and are not restricted to those characteristic of organized crime or serious offenses, despite the avowed purpose of the law.

2. The provision that the application and order shall describe the type of communication sought to be intercepted does not comply with Supreme Court requirements as to particularity.

3. Judge-shopping is possible, and there is opportunity for laxness in supervising interception of conversations.

4. Overhearing of innocent conversations and privileged communications under present procedures appears to be unavoidable and may be constitutionally impermissible.

5. The thirty-day period allowed for listening in, with an unlimited number of extensions each up to thirty days, may protract eavesdropping excessively and violate requirements of the Supreme Court.

6. The law is ambiguous as to who is to be notified of the eavesdropping, who may object, and when motions to suppress evidence may be made.

7. Reports required to be filed are inadequate to inform the public and to form the basis for evaluation of operation of Title III.

Both legal and practical problems are involved in these weaknesses of court-ordered eavesdropping under Title III, and each one of the seven problem areas will be discussed separately.

Offenses Covered

The reason for enactment of Title III of the Omnibus Act of 1968 offered most frequently and with greatest fervor by its supporters was, and still is, that it is an indispensable tool in fighting organized crime. Congress acknowledged this need in its introductory findings in the law. Critics of government eavesdropping insist that the law permits eavesdropping in investigation of many offenses that are not and will not be associated with organized crime. A long list of offenses for which *Federal* officers may seek a court order appears in Sec. 2516(1) of Title III:

- (a) Offenses relating to espionage, sabotage, treason, riots, and enforcement of the Atomic Energy Act of 1954.
- (b) Violation of Federal law restricting payments and loans to labor organizations or offenses in labor racketeering.
- (c) Bribery of public officials and witnesses and sporting contests, unlawful use of explosives, transmission of wagering information, . . . obstruction of . . . law enforcement. Presidential assassinations, kidnapping and assault; interference with commerce by threats or violence; interstate and foreign travel or transportation in aid of racketeering; influencing operations of employee benefit plan. . . etc.
- (d) Counterfeiting.
- (e) Bankruptcy fraud; manufacture, importation, receiving, concealment, buying, selling, or dealing in narcotic drugs, marihuana, or other dangerous drugs.
- (f) Extortion, including extortionate credit transactions.
- (g) Conspiracy to commit any of the enumerated offenses.

These offenses were selected, according to the Senate Report on Title III, because they were characteristic of the activities of organized crime or because of their seriousness (No. 1097, p. 97). However, eavesdropping in any offense seems to be sanctioned on the theory that organized crime has not limited itself to the commission of any particular offense.

The list of offenses in which *State* officials may obtain a court order is shorter, but perhaps even broader than that of the Federal government (Section 2516(2)). The State list appears to be practically unlimited. State statutes may authorize eavesdropping in connection with:

- . . . the offense of murder, kidnapping, gambling, robbery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by, imprisonment for more than one year [or any conspiracy to commit any of these offenses].

Except for the one-year imprisonment limitation in certain cases, the law appears to contain no limitation as to the nature of the offense covered. It may be argued that there is no need to limit the nature of the offenses. On the other hand, it must be recognized that there is great potential for abuse inherent in permitting eavesdropping over a wide spectrum of offenses. The open-ended clause "punishable by imprisonment for more than one year" has been attacked as an inaccurate way of distinguishing between serious and petty offenses.

Have court orders been obtained only for offenses characteristic of organized crime or serious offenses, the avowed targets of Title III? The nature of the offense for each court order granted and a summary of these offenses appear in each annual report to Congress by the Administrative Office of the United States Courts. At both Federal and State level, eavesdropping has been used most extensively in gambling and narcotics cases. Combined, these two offenses accounted for 85 percent of all court orders during 1971 and 1972. The reports do not reveal whether organized crime was involved or the seriousness of the offense. It is possible that many of the targets were small-time gamblers and narcotics peddlers, investigation of whom does not justify costly wiretapping or electronic surveillance.

Congress should take another look at the offenses for which a court order may be obtained. Invasion of privacy of innocent persons is inevitable in wiretapping and electronic surveillance. It may be justified in cases of organized crime and serious offenses where other investigative techniques are inadequate, but not in ordinary cases. Meanwhile, some self-restraint on the part of prosecuting officials and voluntary curbs on indiscriminate use of this powerful tool would seem to be in order.

Specific Offense or Strategic Intelligence

An application for a court order must show that a *particular offense* has been, is being, or is about to be committed [Sec. 2518(1)(b)(1)]. This would seem to limit applications to those seeking specific information about a particular crime—that is, *tactical* as distinguished from *strategic* intelligence. Strategic intelligence consists of general information on the criminal activities of an individual that may enable officials to link him to other suspects or to some specific crime. Is strategic intelligence gathering outlawed by Title III? There is some justification for the view that it is banned. Perhaps Congress should reexamine this problem and attempt some clarification. The use of electronic devices; Committee on Post Office and Civil Service, to obtain strategic intelligence admittedly has great potential for abuse.

Eavesdropping for strategic intelligence is further complicated by Sec. 2517(5) which permits interception and use of a communication relating to an offense other than that specified in the order if the judge finds, on *subsequent* application, that the contents of conversations were intercepted as provided by Title III. The United States Court of Appeals for the Tenth Circuit upheld this provision in *United States v. Cox* [449 F. 2d 679 (1971)]. In May 1972 the United States Supreme Court refused to hear an appeal, over the objection of Justices Douglas, Brennan, and Marshall (*Cox v. United States*, 405 U.S. 932).

For a more detailed discussion of strategic and tactical intelligence, see *Eavesdropping on Trial*, p. 76 et seq. A bill introduced in the House of Representatives on December 7, 1973 [H. R. 11838] appears to deal with this problem, but its purpose and wording require clarification.

The Particularity Requirement

Title III requires that the application and order shall contain a particular description of the *type* of communication sought to be intercepted [Sec. 2518(1)(b) and Sec. 2518(4)(c)]. In *Berger v. New York* [388 U.S. 41] however, one of the two 1967 landmark decisions of the Supreme Court with which Title III purports to comply, the Court made it clear that it was necessary "to describe with particularity the conversations sought," otherwise the officer would be given a roving commission to seize any and all conversations.

In litigation attacking the constitutionality of Title III, it is almost invariably claimed that merely describing the *type* of conversation does not comply with *Berger*. Since it is practically impossible to describe a particular conversation sought, especially in offenses of a continuing nature such as gambling and book-making, the prosecuting official is faced with a real dilemma. To comply fully with *Berger*, the particularity requirement of Title III would have to be narrowly construed, and strict enforcement would make the law practically unusable. Justice Black anticipated the problem of "particularity" in his dissenting opinion in *Katz v. United States* [389 U.S. 347]; he could not see how one could "describe" a future conversation. Justice Douglas has repeatedly observed that it would be extremely difficult to name a particular conversation to be seized and therefore any such attempt would amount to a general warrant, the very abuse condemned by the Fourth Amendment (See *United States v. District Court*, 407 U.S. at p. 333).

What does "type of communication" mean? If all that Title III requires is a statement of the nature of the offense to which the conversation is to relate, then the provision is meaningless, for details of the particular offense have already been set forth in the application and stated in the order. If it means a particular description of a particular conversation, then compliance may be impossible. The meaning of "type of communication" takes on added importance by the requirement in Title III that interception must end automatically when the described type of communication has first been obtained, unless the application shows probable cause to believe that additional communications of the same type will occur later [Sec. 251(1)(d)].

The issue of "particularity" may eventually be settled by the United States Supreme Court. Meanwhile, Congress might effect some clarification by requiring that an applicant for a court order describe the communications sought to be intercepted as specifically and in as detailed a manner as possible. This would discourage the practice of merely repeating the nature of the offense that is being investigated.

Judge-Shopping for Court Orders

A heavy burden is placed on Federal and State judges to whom applications for court orders are presented. Before he signs an order to wiretap or conduct electronic surveillance, the judge must determine whether all the requirements of the law are satisfied. He must make findings as to "probable cause" and decide if the facts in the application show that normal investigative procedures have been tried and failed, or reasonably appear to be unlikely to succeed if tried or to be too dangerous [Sec. 2518(3)(c)]. An order may require periodic reports to the judge showing what progress has been made and the necessity for continued interception. Judges have responsibility for safeguarding the records. The law also gives the judge discretionary power to decide whether certain individuals shall be notified of the eavesdropping, and what portions of the recordings shall be made available for inspection.

The onerous duties and responsibilities of the judge in government eavesdropping make it an unattractive job to sign an order, even for those Federal or State judges who favor this technique of law enforcement. The prosecuting official who wants a warrant to wiretap or use electronic surveillance must find a judge who is willing to issue it and take on all the judicial duties imposed by the law. A wide choice is open to the applicant, for an order may be signed by any judge of competent jurisdiction. This is defined in Sec. 2510(9) as:

- (a) A Judge of the United States district court or a United States court of appeals; and
- (b) A judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire or oral communications.

No safeguard against "judge-shopping" is provided by Title III. Practical necessity forces applicants to pick a judge who is known to be receptive to eavesdropping and at least reasonably lenient in signing orders. Selection of a friendly judge is almost always possible, particularly in State practice. If law enforcement officials can shop around for a compliant and undemanding judge, the dangers of abuse of privacy through eavesdropping may be greatly increased. How is this to be remedied? Competent, alert, and aggressive judges are the key to maintaining the safeguards provided by law.

Congress cannot control the caliber of State judges, or even of the Federal judiciary. It can, however, remedy one obvious gap in judicial supervision of court-ordered eavesdropping: *progress reports* to judges should be *mandatory* and not discretionary. The Act now provides that an order *may* require periodic reports to the judge showing what progress has been made and the necessity for continued interception [Sec. 2518(6)]. Progress reports are intended to serve as a check on the continuing need to con-

duct the surveillance and to prevent abuse. Federal judges are reported generally to require progress reports. Few, if any State judges have specified in the court order that progress reports shall be submitted, although some say that they receive oral progress reports from time to time. This may seriously undermine judicial supervision of the operator who is listening to intercepted conversations and of the law enforcement official who is handling the investigation.

Overhearing Innocent or Privileged Conversations

Congress knew that government eavesdropping would inevitably result in intercepting innocent conversations and tried to deal with the problem. The law requires that "every order and extension. . . shall contain a provision that (it) shall be conducted in such a way as to minimize the interception" of innocent conversations [Sec. 2518(5)]. How is it to be kept to a minimum? The law does not say, other than to limit the time period of interception and to require that it terminate "upon attainment of the authorized objective."

Those who opposed passage of Title III in 1968 were particularly concerned that many irrelevant and innocent conversations would be overheard. Unfortunately, their apprehensions appear to have materialized in both Federal and State practice. Monitoring agents have not been trained adequately to recognize innocent conversations as such and to stop recording them. They simply do not know when to stop listening. Administrative regulations are needed to control the agents who man the monitoring devices. For recommendations of the American Bar Association, see *Eavesdropping on Trial*, pp. 215-216.

The problem of overhearing many innocent conversations is further complicated by the fact that Title III does not state clearly that automatic recording is barred and that live monitoring must be used. In *automatic recording* conversations are recorded on tapes without listeners and are later played back at intervals, the frequency depending on the circumstances and on the practice established in a particular office. The automatic device records *all* conversations. In *live monitoring*, also called "manual recording", police officers or agents sit continuously at the receiving station, listening to the recordings and making notes of relevant conversations on a typewriter or in longhand. The recorder can be shut off when innocent, irrelevant, or privileged conversations are taking place, if they can be recognized as such.

Before 1968, in States where court-ordered eavesdropping was permitted, it was common practice to use automatic monitoring and play back the record at twenty-four-hour intervals. Since Title III requires that a wiretap cease when the conversation sought has been obtained, and that the interception be conducted in such a way as to minimize interception of communications not covered by the court order, it would appear that automatic monitoring is now illegal. Monitoring is done by agents or police officers whose knowledge, judgment, and integrity cover a wide range. Each person interviewed was asked whether he used live monitoring or automatic recording. Those convinced that live monitoring is required by the 1968 law said they always use it. Those who were unaware or uncertain of the need for live monitoring furnished answers indicating that automatic recording is still used (see *Eavesdropping on Trial*, pp. 126-128, 164). This is a matter that could be clarified by Congress. Automatic recording should be banned.

A disproportionate number of innocent conversations seems to have been overheard in some cases; in one investigation reported to the Administrative Office of the United States Courts, 400 telephone calls were intercepted to get one incriminating conversation; in another over 1000 for 20. In a third case 1,342 intercepts were reported to have been made, not a single one of which was incriminating. Even if police officers are instructed not to listen to non-incriminating conversations, no guidelines are available to determine whether a conversation is "criminal"

or not. Some administrative regulations are needed to control extended interception of innocent conversations by monitoring agents. Training programs have been suggested by the Law Enforcement Assistance Administration, but the LEAA's authority to put such programs into effect is limited.

Overhearing *privileged communications*, such as conversations between doctor and patient, attorney and client, priest and penitent, is a problem that parallels interception of innocent conversations, although it does not happen as frequently. Sec. 2517(b) of Title III provides that such communications shall not lose their privileged character whether the interception is lawful or unlawful. This attempt to protect privileged communications does not appear to have been very successful. Most monitoring agents are ill-equipped to decide when a communication is privileged and to stop listening, and the United States Department of Justice is reported to have issued instructions to record all conversations, including privileged communications (see *Eavesdropping on Trial*, p. 160).

Time Period for Interception of Conversations

A court order may allow interception of conversations to continue for a period up to thirty days, with an unlimited number of thirty-day extensions [Sec. 2518(5)]. The time length raises policy as well as constitutional problems. Should it be so long? In *Berger v. New York*, the Supreme Court disapproved of surveillance over a period of sixty days and called it "indiscriminate seizure." In *Katz v. United States*, the Court turned to a case-by-case approach; in this instance interceptions covered a very brief period. A narrow construction of *Berger* would seem to indicate that interception for an entire thirty-day period, particularly with extensions, constitutes a general search and is therefore unconstitutional.

Many State court orders have provided for interception during the maximum thirty-day period, and renewals have been granted freely. Federal orders, on the other hand, have generally limited the period to fifteen days. United States law enforcement officials expressed the opinion that if applications were more conservative than the law required and asked for a shorter period of interception than permitted by Title III, the prospects for sustaining the wiretap in the courts would be improved.

Requests for orders covering a longer period than is necessary frustrate the specific requirements of the law. State and Federal officials claim that an extended period is needed where the offense is a continuing one, but some admitted frankly that extensions were sometimes asked in order to postpone giving notice of the interceptions. It may be argued that the thirty-day period does not square with *Katz v. United States* in which the Supreme Court expressed approval of interception of specific, not continuous, conversations. The granting of an unlimited number of thirty-day extensions also gives rise to the suspicion that a law enforcement official may be engaging in "strategic intelligence" surveillance instead of attempting to obtain specific evidence of a crime.

Congress should reconsider the time period allowed for interceptions in Title III. The conservative section of the American Bar Association (ABA) recommended a maximum initial period of fifteen days in 1971; the more liberal Criminal Law Council of the ABA proposed a reduction to five days, with one extension of five days. The American Civil Liberties Union would like to see all renewals of court orders eliminated. A compromise in reduction in the time period allowed for interception conversations should not be too difficult for Congress to reach.

H. R. 13825 introduced in the House of Representatives by Mr. Kastenmeier with respect to "national security" eavesdropping limits the period of a court order to "no longer than is necessary to achieve the objective of the authorization nor in any event longer than fifteen days." An extension of the order is limited to ten days in H. R. 13825. This would seem to be a reasonable period of time for *all* court-ordered eavesdropping.

Serious ambiguities are created by the provisions of Title III requiring notice of eavesdropping and permitting aggrieved persons to object to the use of evidence obtained. Some injured persons may never be given notice, and it is not clear who has "standing" to object or what should be disclosed. The law requires that notice shall be given no later than ninety days after termination of interception to the persons named in the order or application. In the discretion of the judge, other parties to intercepted conversations may also be given such notice "in the interest of justice" [Sec. 2518(8)(d)]

The purpose of the notice is to give "aggrieved persons" an opportunity to make objections by a motion to suppress evidence. An aggrieved person is defined as anyone "who was a party to any intercepted wire or oral communication or . . . against whom the interception was directed" [Sec. 2510(11)]. Under this definition, an individual may be incriminated by an unlawful interception and yet have no "standing" to object. A person may be "aggrieved," yet the judge may decide that no notice shall be given to him. Furthermore, the notice need not state exactly *what* conversations were intercepted; it is left to the judge to determine what portions, if any, of the overheard conversations shall be available for inspection. The duty of causing service of the notice is placed on the judge, and he may postpone it indefinitely.

Title III is also ambiguous as to *when* an aggrieved person may move to suppress evidence obtained by eavesdropping. Section 2518(10)(a) says it must be made "before the trial, hearing or proceeding," unless there was no opportunity to do it or the person was not aware of the grounds of the motion. Is the motion premature if made before arrest and indictment?

Some of the uncertainties with respect to notice, objections, and disclosure may be clarified by the courts, but this is one aspect of Title III of the Omnibus Act of 1968 that could profit from legislation by Congress. The law leaves much to the discretion of the judge, but the judge really relies on the law enforcement official handling the case. Some officials circumvent the effects of the notice requirement, or at least postpone it, by asking for extensions of the court order. New probable cause as to why the wiretap should be continued must be shown, but this does not seem to be too difficult to do, judging from the number of extensions granted. Judges must rely on the law enforcement officials and appear to be easily convinced that an extension is necessary.

The following proposals deserve serious consideration by Congress: (1) make mandatory the giving of notice to individuals whose wire or oral communications have been intercepted, within thirty days after expiration of the court order; (2) limit the power of the judge to postpone giving notice, particularly where the individual whose communication is intercepted is not engaged in a continuing criminal enterprise; (3) require that persons entitled to notice be given, on request, a copy of the order and application, and information as to conversations overheard. These proposals are included in H. R. 13825 introduced in the House of Representatives by Mr. Kastenmeier on March, 1974 and cited as "Surveillance Practices and Procedures Act of 1974."

Reports on Court-Ordered Eavesdropping

Three reports are required by Sec. 2519 of Title III:

1. Report by the judge issuing or denying an order, within thirty days after expiration of the order or its denial.
2. Report by prosecuting officials in January of each year on each application for an order or extension during the preceding year.
3. Annual report to Congress by the Administrative Office of the United States Courts in Washington, D. C., in April of each year, on the number of applications and orders and a

summary and analysis of the data required to be filed with it by judges and prosecuting officials.

The reports of judges and prosecuting officials, both Federal and State, are made to the Administrative Office of the United States Courts. This Office, in turn, collates the information obtained and renders a report to Congress that is largely statistical. The system set up in Title III for filing reports was designed to keep Congress and the public informed as to the extent of eavesdropping throughout the United States, offenses for which it was used, manner in which surveillance was conducted, identity of prosecuting officials who applied for orders and judges who signed them, cost, and the results of interceptions. It was also to serve as a basis for evaluation of effectiveness of operation of Title III by a 15-member Commission scheduled to come into existence after the law had been in effect for several years. This Commission is now in the process of formation.

All three reports have been widely criticized on the ground that they neither inform adequately nor furnish sufficient data for meaningful evaluation of eavesdropping under Title III. Much of the criticism appears to be justified. Prosecuting officials and judges use a standard form of report prepared by the Administrative Office of the United States Courts to comply with Title III requirements pursuant to regulations issued by that Office. Some of the items in the form of report are vague and convey no significant information. Many law enforcement officials do not take the reports very seriously, and judges are inclined to find them a nuisance and leave the job of filling in the form to the prosecuting official. At least six items in the report of prosecuting officials have been identified as lacking in clarity:

1. *Average frequency of intercept per day.* Suppose during a thirty-day period no interceptions occurred, except on the last day when there were thirty interceptions. Is the average frequency one? How could such an average be of any significance? This item might be improved to require a statement of the total number of days in which interceptions actually occurred, out of the total number of days authorized.

2. *Number of persons whose communications were intercepted.* Does this mean the number of people using that particular phone or calling that number, whether or not their conversations were relevant to the matter under investigation?

3. *Number of communications intercepted.* Suppose calls are made, but nobody picks up the telephone, as often happens. Is the telephone number called to be counted as an interception? I believe that attempted as well as concluded calls should be included.

4. *Number of incriminating communications intercepted.* What is an incriminating conversation? A phones B and says: "I will meet you in ten minutes." Is this incriminating? If one wants to show that many incriminating statements are overheard in order to prove that court-ordered wiretapping and electronic surveillance are effective many calls can be included as "incriminating" that others may find innocent.

5. *Number of convictions.* A conviction may be obtained in a case subject to a wiretap order, but this does not mean that the conviction resulted from the wiretap. Officials should be required to indicate whether conversations intercepted were used as evidence in obtaining a conviction, and whether in their opinion these intercepted communications contributed substantially to conviction. They should also indicate what other investigative techniques were used.

6. *Cost.* Some prosecuting officials find this item so ambiguous and troublesome that they leave it blank. It should be made clear that a statement is required of the exact amount paid to each investigator and all other individuals who spent time on the particular wiretap. It should include cost of equipment, plant, and any other items of expense involved in intercepting conversa-

tions, recording, and making logs and transcripts. Only by strict adherence to this requirement can evaluation of eavesdropping on the basis of cost be meaningful.

The Annual Report to Congress has been useful in publicizing the number of court orders issued, the geographic areas in which eavesdropping (predominantly wiretapping) has taken place, the names of prosecuting officials who applied for court orders and the judges who signed them, and the general nature of offenses involved. Criticism has focused on the summary and analysis by the Administrative Office of: (1) the number of incriminating conversations intercepted, and (2) cost.

The Report to Congress submitted at the end of April 1973 states that "approximately one-half of the conversational intercepts produced incriminating evidence." The report stresses averages; only a close look at each listing would reveal that in one Federal case only 10 out of 500 intercepts were incriminating (2%), and in another case 3 out of 191 intercepts (.015%); in a third, none out of 1,342 (0%). Congress and the public should be made aware of the limitations of the Annual Report and its potential for providing misleading information.

As to cost, the Annual Report to Congress summarizing reports of prosecuting officials and judges for the year 1972 indicated that the cost of an intercept ranged from \$5 to \$82,628, and that the average cost for 805 orders for which cost was reported was \$5,435. What evaluative purpose can be served by such statistics, without relating cost to the results of the intercepts?

No information is included in any report with respect to forty-eight-hour emergency wiretaps without court order or warrantless eavesdropping in so-called "national security" cases.

EVALUATION OF EAVESDROPPING UNDER TITLE III

Wiretapping and electronic surveillance by Government can be justified, according to its supporters, by a *balancing* process. The individual's right of privacy and freedom in a democratic society has to be balanced against the needs of law enforcement and the effectiveness of eavesdropping. Equilibrium is achieved, it is claimed, when official eavesdropping is permitted, with adequate safeguards to protect privacy.

The balance approach to the problem of governmental intrusions into privacy is difficult to apply. To strike a balance between competing interests, the elements on both sides must be measurable and capable of being weighed in similar terms. The right to privacy and freedom, however, does not lend itself to accurate measurement. Nor is it easy to assess either need or effectiveness of eavesdropping in establishing "law and order." What questions must be asked to determine if an acceptable balance has been reached?

As to the *right to privacy*, one must ask whether intrusions against innocent persons have been minimized by the safeguards provided by the law and have been carried out in practice. Some weight must also be given to the potential for abuse inherent in wiretapping and electronic surveillance and to whether Title III has reduced illegal eavesdropping. As to law enforcement *needs and effectiveness* of eavesdropping, it must be determined whether public security has been strengthened by use of Title III against organized crime and serious offenses. Has the law been used against the targets intended, and has it resulted in convictions of top echelon offenders? The sensitivity of the public in a society that places a high value on "freedom" must also be considered in weighing the right of privacy against law enforcement needs, and this depends on who are the subjects of surveillance and for what purpose wires have been tapped.

Minimizing Invasion of Privacy

Invasions of privacy can be reduced to some extent by limiting the duration of court orders to a short period, restricting them to serious cases where less intrusive tools of law enforcement are

clearly not serviceable, and supervising monitoring of conversations closely. Court orders under the 1968 law, most of them for wiretapping, have authorized interceptions for periods that appear excessive; they have been used extensively against individuals in all levels of gambling and narcotics, and supervision of monitoring agents has not been very stringent.

The most careful scrutiny by an impartial judge of applications for court orders, and continued judicial concern throughout the period of the order, are essential if safeguards are to be meaningful and invasion of privacy is to be kept to a minimum. The ease with which it is possible to go to a friendly judge who will sign an order for whatever period a prosecuting officer asks, and the failure of State judges to require written progress reports, leave the door open to unjustified invasions of privacy. The conclusion is inescapable that to the extent that safeguards provided by Title III are ambiguous, the statute as enacted is inadequate in protecting the right to privacy. Insofar as the ideal of continuing scrutiny by an impartial magistrate has not been realized in practice, the protections against undue invasion of privacy have not been fully applied. In balance, privacy has been weakened.

Has Title III reduced *illegal eavesdropping*? The truth is that there really is no way of knowing how much illegal eavesdropping has been going on. Each person interviewed in obtaining data for my study and report on eavesdropping under Title III was asked whether he believed that investigating agents were eavesdropping illegally despite Title III which makes legal wiretapping and electronic surveillance available. Some said illegal eavesdropping was possible, others said it was probable, and a few were positive that conversations not covered by court orders were being intercepted (see *Eavesdropping on Trial*, p. 199). Those who favor eavesdropping under Title III are inclined to minimize the potential for abuse; those who oppose it are sure that illegal eavesdropping is extensive. There is no hard evidence to indicate that Title III has made any appreciable difference either in increasing or reducing illegal eavesdropping, but the temptations for illegal eavesdropping under color of law cannot be ignored.

The Need for Eavesdropping

Opinion has been and continues to be divided on the need for wiretapping and electronic surveillance in law enforcement. Before Title III was enacted in 1968, many law enforcement officials testified in Congressional hearings that eavesdropping was an indispensable tool in dealing with organized crime. Others claimed it was a costly, wasteful, lazy-man's weapon, a threat to innocent persons, and useless against top echelon criminals. No one has ever succeeded in proving need, or even in defining it clearly. Nor has it ever been settled who should bear the burden of proving need. How, then, is need to be weighed in a balancing process? As a start, alternatives to eavesdropping would have to be analyzed, and time and cost factors compared. Would the same resources devoted to normal types of surveillance produce equal or better results or no results at all? If Title III has not been used effectively against organized crime or limited to serious offenses, the need for eavesdropping to promote public safety is weakened in balancing it against invasion of privacy.

Operation of Title III since 1968 has demonstrated neither need nor lack of need for eavesdropping. Nor does the information required to be furnished in reports under Title III further the examination and analysis of need.

Effectiveness of Eavesdropping Under Title III

Has Title III been effective? If it has not, then the balance is tipped in favor of the right of privacy and against wiretapping and electronic surveillance in law enforcement. "Effectiveness" is a vague concept. One factor that Congress seems to have considered significant in "effectiveness" is the number of arrests

and convictions that result from eavesdropping. This item of information must be included in the report of the prosecuting official [Sec. 2519(2)(c)(f)]. But the reports do not show any meaningful relation between eavesdropping and arrests or convictions. If a court order to wiretap has been obtained in a case and eventually a conviction results, does this mean that the wiretap was "effective"? The wiretap may have produced no useful evidence and the conviction may have been obtained on evidence secured by other investigative techniques. The law requires the prosecuting official's report to include "a general assessment of the importance of the interceptions," but the forms examined personally by me revealed that this item is frequently left blank.

Those who favored eavesdropping before the law was passed now claim it is effective. Those who opposed it question the adequacy of the statistics that purport to show effectiveness. Law enforcement officials are inclined to say that arrests and convictions could not have been obtained without wiretapping. Critics of government eavesdropping, however, can always cite important investigations in which it proved to be of insignificant or no value compared with normal techniques.

It can be conceded that eavesdropping has been effective in some cases in obtaining arrests and convictions. This does not prove that other methods of surveillance would not have been equally productive. Nor, in determining effectiveness of Title III, can the quality of an arrest or conviction be ignored. If Title III has been successful in apprehending only small-time offenders and has failed to reach leaders of organized crime, then court-ordered eavesdropping has missed its mark.

Title III has been used most extensively in gambling and narcotics cases. Criminologists claim that the efforts of law enforcement in offenses such as these, which involve willing participants, can have only limited effectiveness, no matter what tools are used. So long as the public wants the services provided and the demand is not satisfied through lawful channels, the illegal activities will continue. Sociologists are inclined to agree; they deplore the tendency of forces favoring government wiretapping and electronic surveillance to deny the relationship between crime, slums, and poverty.

Since *need* and *effectiveness* are such elusive elements and defy accurate measurement, some other factors must be found if the balancing process is used in evaluating eavesdropping. Perhaps one should weigh competing *values*. Is the apprehension of some criminal suspects worth the risks to privacy inherent in eavesdropping? If wiretapping and electronic surveillance are allowed under a law that is ambiguous, and carried on without clear standards and uniform guidelines by a large number of officials in a wide variety of cases without adequate controls, the risks may be too great.

The 15-member "National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance" provided for by Sec. 804 of the Omnibus Crime Control and Safe Streets Act of 1968 (as amended in 1970) has come into existence. The President of the United States has appointed seven members; four members of the Senate have been appointed by the President of the Senate. The Speaker of the House of Representatives has not yet designated the four remaining members of the Commission from the House. The Commission is to file a report within two years after its formation and then go out of existence.

The function of this Commission is "to conduct a comprehensive study and review of the operation of the provisions" of the law in order to determine its "effectiveness." Does "operation" refer only to procedures and practice, without consideration of ambiguities in the law? The scope of the Commission's function does not seem to include the extent of governmental intrusion and whether eavesdropping has been excessive. The "need" for wiretapping and electronic surveillance seems to be assumed; the Commission is instructed only to deal with "effectiveness."

Is the Commission to consider whether Title III has been effective in banning *private eavesdropping*? Effectiveness of the law prohibiting interceptions by private individuals must depend largely on receipt of complaints and vigorous enforcement. State officials report that few, if any, complaints have been received since passage of Title III. Detection of unlawful wiretapping is difficult, and it may be even harder when an electronic device is installed. The Department of Justice appears to have been more active than the States in dealing with private eavesdroppers under Title III, but few prosecutions have resulted. For a discussion of the ease with which the ban on private eavesdropping can be circumvented, see *Eavesdropping on Trial*, pp. 42-43.

Congress should give serious consideration to creation of an impartial unbiased, non-political agency on a continuing basis to oversee government eavesdropping. The commission provided for by Title III has a limited life for a narrow and rather ambiguous purpose, and its composition makes it vulnerable to political pressure. Government eavesdropping has great potential for abuse, as we all know by now. If wiretapping and electronic surveillance by law enforcement officials is to be allowed to continue under law, periodic check of Federal and State practices is essential.

No meaningful evaluation of eavesdropping under Title III can be made by *any* Commission without taking into account ambiguities in the law, lack of clear standards, and failure to establish uniform guidelines; these may create threats to privacy and liberty that are intolerable in a free society. A review of Title III must ferret out information in the field, beyond the statistical data in the reports. In addition to examining whether the protections offered by the law are adequate, it must be determined whether they have been weakened in practice. Modifications are surely needed in both law and procedure.

SUMMARY OF PROPOSALS

Congress has sanctioned government eavesdropping as a law enforcement tool and Americans must live with it—at least until Congress repeals Title III of the Omnibus Crime Control and Safe Streets Act of 1968, the Supreme Court declares it unconstitutional, or the Executive orders its agencies not to use it. Since none of these events is likely in the foreseeable future, the attention of Congress and the public must be directed to minimizing invasion of privacy and maximizing meaningful law enforcement by correcting defects in the law and weaknesses in practice. The following proposals are made with full awareness of the conflict between the two objectives—protecting privacy and dealing with crime—and the difficulties in reconciling them.

1. Clarify ambiguous provisions of Title III, particularly with respect to: persons entitled to notice that eavesdropping has taken place; when motions to suppress evidence may be made; what conversations are to be deemed "incriminating;" what is meant by "type" of communication to be set forth in the application and order; gathering of "strategic intelligence;" use of live monitoring and banning of automatic recording.

2. Limit eavesdropping to organized crime and serious offenses. Perhaps Congress should consider amending Title III to define "organized crime" and "serious" offenses.

3. Establish uniform procedures and standards for Federal and State officials. Automatic recording should be eliminated immediately as a matter of practice, without waiting for legislation to that effect. Progress reports to judges should be made mandatory by law; meanwhile judges should be urged to require them. The time period requested for court orders should be as short as possible, and legislation should be introduced to limit the period to fifteen days, with one renewal of ten days—except possibly on a clear showing that the offense is a continuing one and that additional extension is required. Congress should consider

authorizing administrative regulations to control agents who man the monitoring devices. The Law Enforcement Assistance Administration should be urged to prepare and carry out training programs.

4. Improve reporting requirements. Congress should consider amendment of Sec. 2519 of Title III to clarify the information to be furnished by prosecuting officials as indicated in this Statement. The Annual Report to Congress should also be clarified.

5. Check Federal and State practices periodically. This should be done by a watchdog with no vested interest in the success or failure of Title III. A permanent agency should be empowered to make periodic examinations of Federal and State statutes and procedures, and hold public hearings on law and practice. The inquiries of this agency must be independent and go beyond the statistical reports and summaries submitted to Congress annually.

These are minimal proposals to restore a balance between the right of privacy and law enforcement requirements. Not much more than a year ago, a knowledgeable and experienced member of the House of Representatives estimated that not more than forty Congressmen could be induced at that time to consider any amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968. The prospects for remedying defects and weaknesses in the law in both House and Senate appear to have improved considerably. The public has become painfully aware that widespread wiretapping and electronic surveillance, legal and illegal, are a serious threat to personal liberty. The great potential for abuse and misuse in official eavesdropping has cast its shadow on the purported safeguards provided in Title III. If the law is not clear, if the power of surveillance is diverted to unintended purposes, if it is used indiscriminately for minor offenses, eavesdropping as a tool of law enforcement can be completely lost.

H. R. 9781 introduced late in 1973 in the House of Representatives is, in effect, a reaffirmation of the right of privacy and complete rejection of government wiretapping and electronic surveillance. Banning government eavesdropping may not have present appeal in the face of rising crime, but the pendulum may swing the other way if defects in law and practice are not cured. Clarity in the law, promulgation of uniform standards and guidelines, strictest conformity by officials with all available safeguards, and constant vigilance by Congress, the Courts, and the public are imperative if the right of privacy and the lawful use of eavesdropping as a tool of law enforcement are both to survive.

UNITED STATES SUPREME COURT DECISIONS

Berger v. New York, 388 U.S. 41 (1967)
Cox v. United States, 405 U.S. 932 (1972)
Katz v. United States, 389 U.S. 347 (1967)
Lopez v. United States, 373 U.S. 427 (1963)
On Lee v. United States, 343 U.S. 747 (1953)
United States v. District Court, 407 U.S. 297 (1972)
United States v. White, 401 U.S. 745 (1971)

ANSWERS TO QUESTIONNAIRE ON WIRETAPPING AND ELECTRONIC SURVEILLANCE

1. My name is Edith J. Lapidus. I am a member of the New York Bar and am admitted to practice before the United States Supreme Court. I teach Constitutional Law and conduct a Seminar on the Supreme Court at Queens College of the City University of New York, and hold a Ph.D. degree in Political Science from the City University. My book, *Eavesdropping on Trial*, with a Foreword by Senator Sam J. Ervin Jr., was

published by Hayden Book Company Inc. of Rochelle Park, New Jersey, in February 1974. It presents an analysis and evaluation of the law and practice under Title III of the Omnibus Crime Control and Safe Streets Act of 1968. I believe that at least some of the members of the National Commission received a copy of my book.

I was invited to appear before the Subcommittee on Courts, Civil Liberties and the Administration of Justice, of the House Committee on the Judiciary on April 29, 1974, and prepared a Statement for the Subcommittee on Wiretapping and Electronic Surveillance which was printed in the Hearings held in April 1974.

2. The exception in Section 2511(2) (c) and (d) should be eliminated; wiretapping and electronic surveillance should be banned unless *all* parties to the conversation have given prior consent. In the case of law enforcement officials, a prior court order should be required.

3. The list of crimes for which court-ordered interception may be authorized is too broad and should be limited. It should be made clear that this tool of law enforcement is to be used only in cases of serious offense. In no case should it be permitted without court order. Experience has shown that a court order can be obtained quickly when speed is essential.

4. Electronic surveillance on consent of one party to the conversation should be proscribed. In the case of law enforcement officials, a court order should be required, and reports should be made as in other court-ordered eavesdropping.

5. The Federal system is not too centralized. The State systems are too decentralized; too many law enforcement people at lower levels have been able to obtain court orders based on inadequate supporting documents and to make extensive interceptions under such orders.

6. Yes, there should be greater judicial supervision during the course of a court-ordered electronic surveillance. Written progress reports to judges should be mandatory. Emergency interceptions without prior judicial approval should be banned; the potential for illegal eavesdropping is simply too great.

7. The initial 30-day authorization period is too lengthy. A maximum of 15 days would seem to be adequate, judging from the Federal experience. A mandatory limit on the number of extensions may be unwise, but perhaps judges can be impressed with the need to scrutinize applications for extensions more carefully and make sure that new probable cause is shown. Postponement of notice may be necessary in some limited cases, but judges should be required to justify such postponement. Application for postponement based on affidavits and a court order for postponement may force accountability on the part of law enforcement officials and judges.

8. It may be difficult to formulate fixed standards for minimization of electronic surveillance. A more practical approach may be the training of law enforcement officials to recognize private, irrelevant conversations and to stop listening to them. Automatic recording of conversations should be banned; live monitoring should be required so that the recorder can be shut off when innocent, irrelevant, or privileged conversations are taking place.

9. Explicit court authorization for breaking and entering should be required.

10. A 10-year period for preserving sealed tapes seems to be reasonable.

11. The reports to the Administrative Office do serve some purpose. The trouble is that at least some law enforcement officials and judges do not take them seriously. The seventh report (Jan. 1, 1974-Dec. 31, 1974) observed (p. VIII): "Some judges

appear to be unfamiliar with the reporting requirements." Consensual tapes should be banned. Requiring reports on illegal eavesdropping would be futile

12. Both Federal and State officials admit freely that the law prohibiting so-called "private" eavesdropping has not been effective. The key to dealing with this problem is to discourage consensual eavesdropping and to enforce the law vigorously.

13. Most interceptions of employees' conversations would be eliminated if consensual eavesdropping is proscribed. As to communications common carriers, perhaps Sec. 2511(2)(a) permitting service observing or random monitoring could be clarified, but the real problem is the good faith of the telephone company.

CHAIRMAN ERICKSON: At this time the Commission calls Herman Schwartz.

Professor, will you be sworn?

[Whereupon, Herman Schwartz was duly sworn by the Chairman.]

CHAIRMAN ERICKSON: Herman Schwartz is a Professor at the State University of New York in Buffalo. He is probably the most well known and firmest critic of the use of non-consensual electronic surveillance in law enforcement. He authored an extensive law review article concerning the enactment of Title III which appeared in the *Michigan Law Review*. He has also done studies for the American Civil Liberties Union which seek to demonstrate that non-consensual electronic surveillance has been ineffectively employed.

His analysis of the use of electronic surveillance from 1968 to 1973, based on the data reported by the United States Administrative Office was the background paper for the 1974 Chief Justice Earl Warren Conference of the Roscoe Pound-American Trial Lawyers Foundation and will be the basis of his testimony to this Commission. The report of this Conference was distributed to the Commission members at the end of April 1975.

Professor Schwartz, do you have any opening remarks that you would care to make?

TESTIMONY OF HERMAN SCHWARTZ, STATE UNIVERSITY OF NEW YORK, BUFFALO

PROFESSOR SCHWARTZ: Yes. First of all, I do think that the government of a country as great as ours could do a better job of regulating temperatures in hearing rooms. But I think this is probably an endemic problem with the Federal Government. Federal court rooms have the same problem. They are either too hot in the winter or too cold in the summer.

What I thought I would do is make a few opening remarks summarizing my position.

My position, as I know the Commission is aware, is not exactly a secret. There isn't too much I have to say that the Commission isn't already aware of in one form or another. I have prepared some supplemental testimony which I am sure is boring to everybody which consists of updating the charts that I have. And there are no surprises or secrets in these.

And I have also tried in the testimony to some extent to respond to some special questions that the staff raised with me.

I was shown some correspondence with the Administrative Office of the United States Courts about some of the reporting requirements, and so I have made a few comments about those which perhaps may be of some help.

I was also sent some material on consensual surveillance relating to opinions in Arizona and Colorado. I made a few comments about that.

Also, I made some notes on the testimony yesterday and some of the exchanges, and in particular I made some notes on some comments that Mr. Remington raised. I am sorry he is not here today, but I did chat with him for a few minutes and in the course of my remarks perhaps I might respond to some of the points he made for the record.

My position is, I think, as I say, fairly well known. I appear on behalf of myself and the American Civil Liberties Union, incidentally. They have asked me to appear and give this testimony on their behalf.

It is essentially not that wiretapping is ineffective. I think that is an important nuance that has not been caught in our testimony. Indeed, I don't really know. I suppose it is useful like any other tool, and particularly one that is surreptitious and catches people.

But the case for this extremely dangerous weapon, this extremely pernicious weapon—in my judgment, a weapon which threatens many of the values of our kind of society—has to be that it is more than that, that it is virtually indispensable, that it is terribly important. And indeed that is what all the history of this thing is about.

The legislative history makes it clear this massive statute, which I don't think too much of both from a technical point of view and just over-all policy, is massive because of that, because of an effort which though I think it often misfires and often deliberately misfires, is designed to reflect a community sentiment that this is not an ordinary investigative tool, that this is a special thing with special dangers and special problems for many of the values.

So the burden on the proponents of the tool is more than that it is useful, more than that it is another kind of weapon; the burden must be that this is something that is absolutely necessary and virtually indispensable.

Now, the position that I have tried to support, working from the reports of the Administrative Office, is that in truth it is very expensive and doesn't produce a hell of a lot except in gambling cases, where you put the tap in and you catch a bookie. And you catch a lot of bookies, but you don't catch more than that. And you don't catch very many big organized crime figures.

Indeed, as I have tried to indicate, and as the FBI seems to have accepted now, they haven't caught very many big fish. And as a result there has been a precipitous decline in just three years from 280 or 281 taps during the height of the Nixon-Mitchell administration in the Justice Department, down to 120 in 1974. The concentration is still on gambling, as we know.

And I have tried to lay this out in updated charts. I don't know that there is much point in setting it out in this oral testimony; you see what it is: Over the years several hundred thousand, 200,143 people were overheard; 2.7 million conversations; on the state level particularly heavy surveillance, heavily into gambling, although the states started heavily in narcotics they have shifted over so, as a result, by now some 71 per cent of the total Federal installations over the years have been for gambling; something like 50 to 52 per cent of the state installations are for gambling.

CHAIRMAN ERICKSON: I might interrupt you for just one purpose.

We will file for the record the status of the work that the staff has done on the Nadjari cases that you have referred to prior to the submission of your report. The staff has already gone into that particular case and has checked these out in some detail. I thought that might be of assistance to you in directing your remarks to this particular area.

PROFESSOR SCHWARTZ: Sure. I am not sure I had planned to say very much about it except what is in here. I am hoping not to duplicate what is in here because it will be on record anyway.

The staff has kindly furnished me with this document which contains many surveys.

Has the staff gone beyond what is in here?

MR. STEIN: Not in Nadjari matters. We will be inquiring into the length of the taps and investigations.

PROFESSOR BLAKEY: Mr. Chairman, it is my understanding that all taps of that character, not just the one of Mr. Nadjari's office, are being gone into; is that correct?

CHAIRMAN ERICKSON: In depth.

PROFESSOR BLAKEY: And the report that is in the record at this point will cover all of that material?

PROFESSOR SCHWARTZ: What is all of that material?

PROFESSOR BLAKEY: It is my understanding, Professor, that as a result of prior discussions in the Commission the staff is making an effort to examine all court-ordered wiretaps since 1969 to see the length of time they ran, the number of incriminating conversations and the probable results. Those taps which raise a question on their face are being examined to determine why they were put in, who supervised them, what the attitudes of the judges were. This is, I think, relevant to the point you make about at least the one situation with Nadjari.

PROFESSOR SCHWARTZ: I think also some of the points I have tried to make have to do with the cost of this instrument. I was particularly pleased to see that in the staff report, there is a conversation with the Special Attorney for Narcotics, Mr. Frank Rogers, who seems to disagree with the view of the Administrative Office of the United States Courts. The Court says that it didn't include lawyers' time and that kind of thing and it doesn't think that would be significant to the cost and it is one of the limiting factors on his use of electronic surveillance.

The cost per person convicted for what I tried to work out on the Federal area was something like \$3,500-\$3,700 per person convicted.

And I was also interested in noting that the staff report shows relatively little judicial control, which is what one would have expected.

And with respect to results, again my figures show what I would refer to as a great many dry holes. An awful lot of this stuff just doesn't turn up much of anything, and when it does, a lot of it is pretty small fry.

I remember one case in particular, the *Whitaker* case, which I handled in the Court of Appeals. And the reason I handled it in the Court of Appeals is there were some five or six defendants in that case. And five of the six, if there were six, or four of the five, were such big fish that they couldn't afford to appeal from a decision in their favor and therefore they asked whether the *amicus* brief I was going to file couldn't be in their behalf rather than *amicus*.

PROFESSOR BLAKEY: Do you mind if I make a comment?

PROFESSOR SCHWARTZ: Yes.

PROFESSOR BLAKEY: The *Whitaker* case is not unknown to me. I was in the Department of Justice and in 1962 or '63 I prosecuted him at the time.

PROFESSOR SCHWARTZ: I know it.

PROFESSOR BLAKEY: Both for interstate gambling and tax evasion.

PROFESSOR SCHWARTZ: You got nine months on him.

PROFESSOR BLAKEY: And he pled guilty to the tax evasion. Our investigation into his numbers and bookmaking at that time warranted, if I remember correctly, a \$900,000 jeopardy assessment. I am not sure how the thing came out, whether they actually collected that from him, because I know he was very careful in hiding his assets.

And just for the record, I would suggest to you that, while he may have qualified for an indigent brief, based on the investigative work we did on him, he was anything but indigent.

PROFESSOR SCHWARTZ: He wasn't one of the five or six. He had his own lawyer.

PROFESSOR BLAKEY: Most of the people you worked for were not terribly well paid and could easily have qualified as indigents.

PROFESSOR SCHWARTZ: And when one looks at the convictions those will fall into the convictions as five or six. I am not saying one doesn't get a big fish once in a while, but I am saying these numbers are swelled by a number of these—which the FBI has admitted when they said last year they were going to cut down on their tapping and move from quantity to quality. I am not sure that has happened. It takes two years for these cases to get through the process and we don't know in all honesty what has happened.

It is very gracious of you to mutter "nothing."

And my point is, as it has always been since 1967, not only was all of this predictable, it was predicted and known. Because the whole point of this operation is to get strategic intelligence and I don't think the Constitution allows that. Indeed I think Mr. Justice Powell, in the *Damon Keith District Court* case, raised the possibility that it might be allowed but said there has to be specific Congressional approval. At the Roscoe Pound Conference to which you referred, Mr. Chairman, a representative of the Justice Department said, "Well, of course not, we never could have gotten the bill through if we told them all we were going to do was go after gamblers to get strategic intelligence." And that was known at the time and I think has been known to those of us who followed it closely.

I think that is pretty much all I want to say about my general position; you know it and I have simply reiterated it to get it on the record.

CHAIRMAN ERICKSON: Your statement and the articles that you have referred to will be included as part of the record.

PROFESSOR SCHWARTZ: Yes, and I assume for whatever it is worth, it will be considered.

CHAIRMAN ERICKSON: Your reputation.

PROFESSOR SCHWARTZ: I was asked to look into the special case of Maurice Nadjari and in all

honesty I think it is a little early. He hasn't been around much. He hasn't done much in the time he has been around. His two biggest convictions—and I don't know whether electronic surveillance had anything to do with it—were Thomas Mackell and Norman Levy. Both got thrown out. In both cases I think leave to appeal has been granted by the Court of Appeals—certainly in the *Mackell* case; I am not sure about the *Levy* case.

And he hasn't done much. There has been a lot of criticism of him for that.

And we do know that wiretapping is an essential part of his operation. Indeed, he reflects an attitude I was told about many years ago which is reflected in the reports of the whole New York operation in general, particularly those coming out of the Rackets Bureau, what many of us will always refer to as Mr. Hogan's office.

And that is a story that was told to me by a man named Jerry Cohen who some of you may know who was Chief Counsel for Senator Hart's Antitrust Committee. Cohen went to an organized crime seminar in New York—or some kind of thing like that—that was given by the Hogan office. And he told me the first thing that was said was, "The first thing you do is put in a wire." And he said, "Wait a minute. We can't put in wires, at least not legally." The response was, "Then there is no point in talking about anything more."

And that whole operation is built around the assumption you can't do anything any other way. That is the basic mode of thinking and it goes back to Thomas Dewey and it seems to me that it is a very difficult task to make judgments about whether that office would or would not have gotten the convictions that they did get, assuming that they have done a good job, without wiretapping, because you just don't know how to deal with contrary-to-fact conditions; you just don't have anything to work with.

So I think with respect to Mr. Nadjari, while we do know he has spent a lot of money, done a lot of tapping—he hasn't gotten much yet.

Interestingly enough there is an ambiguity, or at least a slight confusion in the statistics. The fact is that his heavy wiretapping, if the reports are accurate, was in 1973. He had 24 in 1973 reports, and 32 in the 1974 reports. But of the 1974 reports, 12 are from 1973.

Now, I don't know whether that means we will get the same thing next year—in other words, latter half-year reports in '75—but if we don't, what that means is that he has substantially tailed off on his electronic surveillance as well, and I don't know whether we will know the answer to that until next April.

Now, I went through the staff reports and found them absolutely fascinating—partly, of course, because they confirmed a great many of my own predispositions, predilections and what some of us charitably call prejudices.

In the first place, I found that the problem of corruption is not an unimportant factor, police corruption in the whole wiretap situation. And one of the problems with wiretapping is that it concentrates precisely in the areas where police corruption is greatest and most troubling: gambling, and to a lesser extent narcotics.

Secondly, at least three of the reports commented that wiretapping is really not of very much value for such things as loansharking—the Brooklyn reports, the Bronx reports, and one other.

Thirdly, interestingly enough in connection with the comment Chief Andersen or somebody made yesterday to Judge Stern about corruption and wiretapping in connection with corruption, the interesting thing there is that the New Jersey State Prosecutor's Organized Crime Special Group has very sharply decreased their use of wiretapping, one of the explanations being that they have shifted from gambling to corruption and wiretapping isn't much use in corruption cases, they say, which would seem to bear out Judge Stern's comments that at least he didn't find it terribly useful or necessary to do that.

There was also, what will surprise no one, fairly clear evidence that the court-ordered system doesn't amount to much as a screen and certainly not as a supervisory level—on the state level.

[All my comments on the staff reports will be on the state level of tapping, because I don't know if the staff has made a study of the Federal tapping in this form, but this volume was limited to the states.]

Another thing that came out is that the penalties are pretty small potatoes. It is very rare that one finds much above a year—an occasional reference to four years which, in my state in any event, is the lowest felony. A Class E felony is a four year maximum. I don't know if the conviction was of higher offense and that was the penalty imposed, but that was the highest.

There are a fair number of suspended sentences referred to, also.

Places like Rochester and elsewhere seem to come to the conclusion that it isn't terribly helpful.

One of the most troubling aspects, of course, about the whole wiretap controversy and that which has troubled many of us particularly, is the fact that even if New York County, perhaps, handles it wisely, even if the Special Attorney handles it wisely, even if the New Jersey Organized Crime Section handles it wisely, you don't write a statute

for those people. You write a statute for the District Attorney in Niagara County near me who used the wiretap statute for Peeping Toms. You write it also for people who use it against prostitution, who use it to build up a box score against very petty gamblers, local bookies and the like.

I was also struck by an interesting comment. In the report on the New Jersey Attorney General dealing with organized crime, in the staff commentary on page 3 of one of the case reports, it indicates how very difficult it is to reach top figures in organized crime who are cautious. This leads me to a couple of passing comments on some of the papers that were submitted earlier from Los Angeles and Chicago, which I skimmed through this morning, in which we find comments about, "How nice it would be if we had wiretapping because we might have been able to get information."

But of course one never knows that. And if there is wiretapping in a state, it may be the very people who you want to get will become very much more cautious and therefore you won't get anything except an awful lot of invasions of privacy.

Now, I should like to make some comments, in closing what I think laughingly can be called my prepared statement, with some remarks on some of the things that were said yesterday.

Let me first turn to the question raised by the chairman about expectations of privacy, whether we have any expectations of privacy on the telephone. I hardly need mention that the key Constitutional phrase is "reasonable expectation of privacy" not "expectation of privacy," as used by Justice Harlan in his concurrence in *Katz*, and that has been used there and elsewhere.

And the statement "reasonable expectation of privacy" has a top side and bottom side. The bottom side is that not everything will be considered. But it also has a positive top side, which is that there are some things we are entitled to consider, that a free society does not say that because the police break in a lot that, therefore, you don't have an expectation of privacy.

Senator Ervin raised this issue with Mr. Ehrlichman about the break-ins, about whether this wasn't a violation of the Fourth Amendment. And I do hope and I assume that the Commission will not adopt the response of Mr. Ehrlichman, paraphrasing him, "Well, the Fourth Amendment has been eroded a good deal in recent years."

The reasonable expectation of privacy that we have applies to the telephone—

CHAIRMAN ERICKSON: I might say I don't think Mr. Ehrlichman's statement either stands as an interpretation of the Fourth Amendment by the Supreme Court or by any recognized authority.

PROFESSOR SCHWARTZ: No, except I think that as a fact now it is true. The Fourth Amendment has been eroded, but not as a statement of Constitutional law. I quite agree with you.

PROFESSOR BLAKEY: Professor, would you rather say it has been violated and not eroded? I would like to say the Fourth Amendment is still all right; it is the people who don't believe in it that give us the problem.

PROFESSOR SCHWARTZ: We may take a different position on that. Because I think it has been eroded by people who believe in it in such areas as "Stop and frisk," and in certain border search areas—which gets us somewhat far afield, and unfortunately, both being professors of criminal law and criminal procedure, I am afraid we tend to drag everybody else with us as we tend to go off into tangents willy nilly.

But I think there has been erosion in the last six years since 1968, and that is sort of what I have in mind. I don't think Mr. Ehrlichman had in mind anything quite as rarified as that.

But in any event, let me go on from there and also comment about expectations of privacy in jails.

And I don't know how the chairman meant that yesterday, but nothing could better illustrate my point. There isn't much of an expectation of privacy in a jail, in a prison. It is as close as we come to a police state. And I would hope that that is precisely what we will try to avoid.

And in that connection, also, I think it is relevant that the fears expressed by Mr. Clark yesterday, which I share completely, and to some extent we are talking about a series of footnotes to his testimony—is a fear that I think this morning's newspapers amply justify, and which the FBI has deliberately fostered.

I am sure the Commission will remember the statement found in a newsletter in the Media papers, a newsletter to FBI people, saying, "Let us make it clear that we have informers around, which will enhance the paranoia endemic among these types of people in society."

And certainly when one reads about the kinds of CIA infiltration into such things as the Southern Christian Leadership Conference, the American Ethical Society, the Urban League, Women's Strike for Peace and 12 other organizations, it doesn't take much paranoia. It simply becomes hard-nosed reality to feel that this kind of stuff is just all over the place and that includes wiretapping and bugging.

Now Mr. Remington raised the question here yesterday if the fear here is not perhaps a class fear—

CHAIRMAN ERICKSON: What is that?

PROFESSOR SCHWARTZ: A class fear. And he raised the question about how this was to be compared with arrests. He said, "If I had the choice between being wrongly arrested and being overheard wrongly, I think I would prefer being overheard improperly."

I don't know how one draws those distinctions, but I think I would, too, depending on what I was saying on the phone but for most of my phone conversations I think I would rather have them overheard rather than have somebody in a blue uniform say, "Up against the wall, Buddy," and pat me down.

But I don't think it is a class factor because the key difference between most arrests and the wiretap situation is two-fold.

First, the arrest is relatively specific. When it doesn't remain specific, as happened on May Day in 1971 or '73—I have forgotten, then you have the *Davis v. Mississippi* kind of situation, when it is not specific, and it is clearly unconstitutional.

And, secondly, there is a link with speech. There is no way to limit wiretapping to things involving organized crime, assuming it was particularly useful for that. Every statute which allows wiretapping is going to allow it for sedition and everything else. And the people who fear wiretapping are not just upper middle-class academics or members of the ACLU, but members of dissident groups of various kinds, and many of them at the bottom rung of our social ladder in various ways—blacks, Indians and the like. The Rap Brown Act was, after all, called the Rap Brown Act. It wasn't called the Dr. Spock Act or anything like that. It was aimed at black militants as well as at middle-class "New Left" types.

And therefore I don't think the concern is solely that of intellectuals and the like, but it is the concern of anybody who thinks that he may be involved in an activity that those who run the show aren't very happy with.

Now a question was also raised about the emergency possibility and just a footnote—indeed a reference to a footnote—of Mr. Justice Stewart in the *Katz* case—I forget whether it is Footnote 16 or 23—which said specifically that it was very difficult for him to see how the normal Fourth Amendment emergency provisions of exigent circumstances and the like could ever apply to wiretapping.

And indeed the New Jersey situation deals with precisely that kind of situation.

California allows warrants by phone, and I wouldn't see any problem with that, either, a warrant by telephone. Because, as Judge Leventhal, I think, has indicated in several decisions, the key factor in many of these cases is simply to get a con-

temporaneous record of what the investigators thought they had.

PROFESSOR BLAKEY: Professor, would you mind a question at this point. Would you feel satisfied with a provision that said it must be initiated contemporaneously, that is the court order process must be initiated contemporaneously with the installation?

PROFESSOR SCHWARTZ: No, I think you can catch a judge. It isn't that hard.

PROFESSOR BLAKEY: And fill out the complete affidavits contemplated by Title III?

PROFESSOR SCHWARTZ: One can put into a telephone and a tape recorder at the other end—with consent, I assume, and probably with a warrant as well from that judge—one can read into a tape recorder the information one has. It can take five minutes, three minutes to say, "We have gotten information that there is an assassination possibility," or what have you. "There is one chance in ten thousand."

PROFESSOR BLAKEY: Would you be willing to see a kind of "good faith" amendment provision added to the Act?

PROFESSOR SCHWARTZ: Of course. It doesn't have to be technically correct. The Supreme Court has said it is not the affidavit—

PROFESSOR BLAKEY: Suppose in making it out you inadvertently leave out a whole paragraph that would be essential in an affidavit, all other things being equal. Would you permit it to be amended at least as to that paragraph error?

PROFESSOR SCHWARTZ: If I could be sure that the amendment was not a reconstruction of something that hasn't taken place.

PROFESSOR BLAKEY: I suspect that could be an issue for litigation.

PROFESSOR SCHWARTZ: I think so. I am not sure. I haven't given the matter that much thought. But it seems to me the key factors are the essentials of what you need for probable cause. The key factor is to make a contemporaneous record and to have a neutral person look at it right away and say, "Is this a hunch or is it something more?"

It is done in California apparently without too much difficulty.

PROFESSOR BLAKEY: But it is your testimony that you would be willing to have a kind of "good faith" amendment?

PROFESSOR SCHWARTZ: I think so.

PROFESSOR BLAKEY: If you do so, say so, so there is no disagreement.

PROFESSOR SCHWARTZ: I'm not worried about disagreement.

PROFESSOR BLAKEY: No, but I am saying the people who press for a kind of emergency authority

assume beforehand that it is not possible to fill out the affidavit and get it to the judge in time to make the meet. What you are suggesting is that you give them a telephonic procedure and you give him "Sony reporting" rather than an affidavit, and you may even give him an opportunity to amend it later.

You know like I know Mr. Justice Jackson, who was the Solicitor General before he sat on the Supreme Court, once described as the most able advocate that appeared before the Court and was, said that he always made three arguments: the one he thought he was going to make; the one he made; and the one he wished he had made.

So I am saying in the press of the investigation the officer will, the day after the affidavit was submitted, think about something he should have put into it and had he had more time he would have. And it may very well be in his records that pre-exist the surveillance, so there can be no question about reconstruction.

And if you are willing to recognize that kind of flexible procedure, then—

PROFESSOR SCHWARTZ: I am nervous about it and the reason I am nervous about it is because I have very little reliance on the police to refrain from making up after the fact something that they think will meet the Constitution.

And I add to it what I have read only in short excerpts in the casebook that I use, which may also be the one you use, but in any event a description of the California experience with telephone warrants, which doesn't seem to need that kind of thing.

But I don't know enough about the operation of that system, I don't know enough about whether it does include this kind of *post hoc* amendment—

PROFESSOR BLAKEY: It does not. But what you are dealing with—

PROFESSOR SCHWARTZ: If it doesn't and if they manage to survive, then I think I am very resistant to it, especially since I think the emergency business is nonsense. I don't know of a single Federal emergency situation and I know of very, very few state emergency situations. And it is my experience that it just isn't that hard to get a judge, to find a judge, to have somebody appear before the judge. I have appeared before a Federal commissioner late at night.

We are really not talking about, in most cases, somebody way out a hundred miles from the city. We are often talking about urban police officials. It is not that difficult to have a magistrate or a judge on duty, rotating all the time.

You know there is a scandal in our own state about a judge who suddenly appeared at 3:00 a.m. to provide bail for somebody.

I am nervous enough and distrustful enough to say that I would settle for what they have in California to start with as an experiment for the emergency case, without opening it up more.

Perhaps that shows a certain inflexibility, but I think this is an area where I think we have been burned badly.

CHAIRMAN ERICKSON: Let me ask you this on the emergency issue.

Have you examined the Canadian statute which has emergency provisions which seem to be a little more useful than ours?

PROFESSOR SCHWARTZ: All I can say is I know about it. I have read some newspaper reports, but I haven't examined it.

I noticed, also, that a lot of the convictions or a fair number of the convictions particularly in the New York area are for contempt, perjury. And I really find these very, very troubling kind of convictions. Perjury and contempt are used when you don't have much of a case. And when you call somebody before a grand jury and you know they are not going to talk, it seems to me that there is some question as to whether that isn't an abuse of the process.

And I find that is true in a fair number of the New York convictions.

Finally, Mr. Blakey asked yesterday what seems to me a very profound question of Mr. Clark. I didn't like the answer that you were leading toward, but I thought the question was really a very important one.

You asked whether it is impossible to have crime control and concern about social issues.

In a way, that problem has dogged this country in various ways for ten years. It is a variation of the guns and butter argument we heard in the mid-Sixties, why can't we have guns and butter? And President Lyndon Johnson, of course, said we can have both.

And the answer is that although it would be nice to have both, as a practical matter—and we have seen this in the economy today and I think it is true in the area of the social problem known as crime control, crime rates—I think the answer is we cannot have both or at least a preoccupation with the gun side means, as a practical matter, we don't have the other. We haven't had many social programs in the last six or seven years.

PROFESSOR BLAKEY: We haven't had much crime control, either.

PROFESSOR SCHWARTZ: But we have had the guns. We have had this Act. We have had a lot of money poured into the states. We have had a lot of money pouring into crime control.

Maybe what that means is that we are going about it the wrong way, but nevertheless the result of it has been that we certainly have not gotten much social butter in the area of crime control. We have gotten a lot of guns.

I think that is all. Oh, I think my comments on the Administrative Office questions are in my report. I have asked and suggested that they could refine some of their figures in ways that I don't think involve that much more work. And certainly if they go to computers, whether it is in the Administrative Office or somewhere else, a lot of this stuff is very, very easy to develop—certainly breakdowns between Federal and state. I have never really understood why, when they start breaking down the Federal, they force us to use pen and paper and do a lot of addition and subtraction to figure out the state implications and components.

On consensual eavesdropping I notice the committee has asked a lot of questions. I think my position on it is set out, both in the Roscoe Pound paper and in my statement here, which is that I think that it really deals much more profoundly with the problem of informers and betrayal, rather than with electronic surveillance.

And I think that the questions that the chairman asked this morning are very troubling questions, because the truth is that in a lot of these cases—and I don't know how to resolve this problem—in a lot of these cases you just couldn't get a warrant, certainly for the initial kind of infiltration. So you come down to the question of what do you do? You say you don't have it at all?

And I don't have any answers to that. It is my impression that law enforcement really finds informers an indispensable tool, in my sense of the word "indispensable," that it really needs informers. And how you control infiltration into political organizations, I don't really know.

But I do know this: Once you have electronics enter into the picture—and I have drawn a distinction here which no one else is willing to buy—including my colleague, in the loose sense, Kent Greenawalt—between the *White* situation and the *Lopez* situation. No one else buys it. It seems to me a transmitter is different from a recording machine in various ways.

Anyway, it seems to me that unlike the loose infiltrator, once you put a wire on somebody you are zeroing in. You aren't in a situation of just general fishing, whether that is good or bad. And I think a warrant system for that area could be devised. It is clearly not constitutionally required. Nothing could be clearer, I think, from the Supreme Court's repeated and emphatic statement about this that it is not constitutionally required, but obviously social

policy and legislative policy, I would hope, goes beyond the constitutional minimum, and I would hope this Commission might recommend that.

I don't know that I have very many expectations of that, reasonable or otherwise, but I think that it is feasible; it is workable. And I think it probably should be done.

One final comment. I am not sure the recording is that much more accurate than the people's recollections. In many cases these recordings work very, very erratically, the recording machines, and often there are an awful lot of gaps in these things.

I recall a story about the *Berger* case. The case was tried in 1963 and there was a clipping in the *New York Times* to the effect that the week before the day—the day before the case went to trial—the prosecutor and the police were still trying to reconstruct parts of the transcript, listening very, very closely, and there were still big gaps in the transcript of what was overheard on the tap.

I didn't mean to filibuster. I am at your pleasure.

CHAIRMAN ERICKSON: I believe to rectify this, Professor Blakey has a few questions that might lead us into other areas.

PROFESSOR BLAKEY: Professor, I really want to welcome you to the Commission. As you know, but perhaps some of our readers might not know, our conversation about wiretapping and electronic surveillance is not a short one. I believe we first met in 1965 and at that time began to discuss this problem, we have been discussing it ever since—

PROFESSOR SCHWARTZ: I might say it is the Tenth Anniversary.

PROFESSOR BLAKEY: It is almost the Tenth Anniversary of the conversation. I also must express my regret to you that more of our fellow Commissioners aren't here. We have committed the unpardonable sin that was first committed at the marriage feast; we have saved the best wine for the last. I hope that my fellow Commissioners will read your testimony and I am sure that those who read our record will feel that this is probably what they have been waiting for.

Let me discuss with you what runs through so much of what Attorney General Clark said yesterday and was one of the major points you raised today—and, frankly, the one that troubles me most. That is not the Fourth Amendment, not the Fifth Amendment; it is the First Amendment.

The one objection that I have the most difficulty with in the electronic surveillance is the First Amendment.

If, indeed, wiretapping seriously inhibits, through fear of surveillance, free speech, maybe the game is not worth the candle.

Yet don't we have to make distinctions dealing with the source of the fear? If we legally banned all law enforcement wiretapping tomorrow in the domestic area—let's forget the international security area—do you think this would substantially change the fear on the part of dissidents in our society that they are being wiretapped?

PROFESSOR SCHWARTZ: I don't know the answer to that. Judgments about such massive social phenomena are very, very hard to make.

PROFESSOR BLAKEY: I take it that most of the wiretapping that has occurred against dissidents that we know about was on the most generous reading—and I underline the word "generous"—national security tapping.

Any honest analysis would say it is an outrage.

And it is not an unfair characterization to say it is illegal.

In other words, it is outside of any scheme that we thought would be permissible—

CHAIRMAN ERICKSON: Professor Blakey, I wonder if you would mind turning your microphone up a little bit toward your mouth. We are having some difficulty hearing you.

PROFESSOR BLAKEY: You see where I am going?

PROFESSOR SCHWARTZ: I share your views, obviously, about the Martin Luther King thing—and of course it is not unique.

I think something happens to a society—and here I am just sort of generalizing and I don't know precisely. I don't know how one measures such social phenomena. Like everything else, what one sees is what one looks for.

I think something happens to a society in which intrusions on intimacy, surreptitious intrusions on intimacy are legitimate, become rooting, that I think is not a good thing.

I think, for example, that having the equipment around, having it legitimately available, enhances the "paranoia endemic" to these kind of people.

PROFESSOR BLAKEY: We can categorize the kind of surveillance that is being done as national security—

PROFESSOR SCHWARTZ: No, I am not talking about national security.

PROFESSOR BLAKEY: Let me go through the basic categories. International and national security—and I think there is probably no realistic possibility that our society will cease doing that. It may be a better thing to do. Attorney General Clark has testified that it is no good anyway, but it seems almost anyone who makes a statement about it, except people with courage, perhaps such as yourselves, say we want no tapping, with the exception of national security.

The next field is national security domestic, which is today illegal.

PROFESSOR SCHWARTZ: What did you say?

PROFESSOR BLAKEY: Which is illegal. And I think realistically, there is no possibility that this Congress or one in the next decade is going to authorize some kind of domestic national security surveillance under anything except Title III.

So the three categories we are talking about are illegal surveillance by private groups, illegal surveillance by the police and the court-ordered system.

Is the fear people have of surveillance related to the illegal categories?

Can't we build into the court-ordered system such things as the annual reports and inventory procedures to reasonably assure people this is not being used for the suppression of political dissent?

PROFESSOR SCHWARTZ: I don't think so. Because I think the distinctions you draw, though analytically absolutely sound, of the three categories that remain once one pushes those out—I think those distinctions don't affect practical life.

I think what happens is we are known now as a 'bugging' society, a 'tapping' society, where this kind of thing is legitimate. And I am just paraphrasing Brandeis here. After all, we are talking about something which we all agree is by and large an intrusion—the legislative findings preparatory to Title III say that—an intrusion into the intimacies of people's affairs. We are talking about something that—I don't know about members of this Commission, but I think it is fair to say that a vast number of people in America believe—even those who support law enforcement surveillance—believe to be a bad thing.

The polls, the few polls that have been taken, are startling. They show that an enormous number of people oppose all electronic surveillance, even for serious offenses. And, of course, it is not used for serious offenses by and large.

And when a community says that 'despite our distaste we are going to allow this kind of stuff because the end justifies the means'—and there is nothing wrong in the end justifying the means but you have to realize what price you are paying for those things. When that happens, it seems to me you have seriously degraded the nature of society.

So therefore, although I think the analytical distinctions you make are sound analytical distinctions, to try to refine out causal links with respect to, as I say, such vast amorphous social phenomena as the quality of the society and the, quote, 'sense of paranoia,' is just too difficult.

PROFESSOR BLAKEY: Can't you draw a distinction here between legitimate fears and illegitimate fears?

Let me kind of run this by you and see what you think about it.

If we decide there is indeed fear today both of the court-ordered system and illegal practices and this is impeding the First Amendment freedoms, and we decide that the history of the last four or five years, as I understand it, indicates serious abuse in the illegal area and indeed abuse in the Federal area, but interestingly enough, none of that kind of maliciousness in the court-ordered system, has the court-ordered system been used to abuse personal rights?

As I understand it, it has not.

If that premise is correct, wouldn't our remedy be rather than abolishing the court-ordered system to meet the fears of the people, rather to engage in an honest effort to show people there is a distinction between illegal wiretapping and court-ordered wiretapping, and the court-ordered wiretapping, if carefully designed, does not threaten First Amendment freedoms.

Once people understood what was involved, then the fear could be properly confined to the illegal area, and if we could focus the social opprobrium on it, focus community sentiment on it, maybe we could cut it down.

PROFESSOR SCHWARTZ: Let me indicate some of the problems I see with that.

You state that there has been no abuse of First Amendment rights of protest, rather than speech association and the like, on the court-ordered side.

You know, part of our problem has been that after all of the talk about the importance of wiretapping to national security offenses, national security, and the like, we don't have any reports of any wiretapping in that area. Why? Does that mean they don't do it? Not at all.

It seems to me that means they have been doing it under the national security intelligence rubric. Because, in case after case involving prosecution, we find there was a wiretap in there.

I have no reason to think that is not continuing.

Now, if we ever seriously manage to eliminate intelligence surveillance—ignoring for the moment the foreign national security stuff—who knows what may happen in Title III tapping?

At the moment there has been no need to move into that area in Title III, and so they have concentrated on the Federal level almost exclusively on the gambling and drugs and the rest.

PROFESSOR BLAKEY: But—

PROFESSOR SCHWARTZ: Let me continue and turn to the states now.

There is an awful lot of drug tapping on the state level.

It is my experience that in many, many jurisdictions the drug squad is also the racket squad—certainly in my area. And the drug culture, as we know, is very close—the counter-culture—to the political dissent culture.

I haven't checked some of these drug taps, but I think I would have to disagree with Professor Lapidus who said she didn't think marijuana would be included in the statute. It is quite explicit. You don't need that danger to life, limb, and property. And I know there have been marijuana taps on the state level.

Now, people that I know on the, if you will, left or political protest, know very well you don't need to go and get a warrant for political surveillance or for a violation of the New York, whatever it is, anarchy act or something like that. You don't waste your time with that stuff. You go get a drug warrant because certainly where marijuana is concerned, it is not very hard to get probable cause for a warrant that somebody is possessing or selling or transferring marijuana.

PROFESSOR BLAKEY: But—

PROFESSOR SCHWARTZ: Let me just finish the sentence—or finish the paragraph.

PROFESSOR BLAKEY: But not the chapter.

PROFESSOR SCHWARTZ: Okay.

I don't think the distinctions you draw are workable in practice. That is the bottom line of what I am saying.

PROFESSOR BLAKEY: Couldn't we make, among our recommendations, one for public education, as to the nature of what is going on—indeed, this Commission's report and its hearings should hopefully perform a substantial public education function.

PROFESSOR SCHWARTZ: I would certainly hope and suspect that.

PROFESSOR BLAKEY: One of the things we have talked about recommending, the necessity for lawyer-investigator teams to guarantee that there is a greater infusion of law-trained people into supervision of wiretapping and to guarantee that the ethics of the officer of the court will begin to filter down into the efforts of investigation—perhaps one of the recommendations that could come out of this kind of colloquy is that we should specifically recommend, for First Amendment reasons, that those agencies authorized to do court-ordered surveillance not have subversive responsibilities; that there be a clear separation of the subversive squad, if indeed there should be one in major metropolitan areas, and the organized crime and vice squad.

Moreover, it may well be we could say the First Amendment dangers of marijuana surveillance would justify it not being one of the crimes in the wiretap statute.

What I am saying is: How many specific amendments could we make to the system short of abolishing it that would meet the First Amendment objections?

It seems to me that the First Amendment impact is not a per se objection to the statute. It is rather an unfortunate tendency of it in our society today.

PROFESSOR SCHWARTZ: Well, I think my answer to that is that the First Amendment objection is an objection to the use of electronic surveillance per se. That involves more than political speech. It involves social speech, commercial speech of various kinds.

PROFESSOR BLAKEY: But it doesn't involve criminal speech.

PROFESSOR SCHWARTZ: But you are not limiting your stuff to criminal speech. Part of the problem is it catches all kind of speeches.

One of the major problems—and I notice Dick Uviller made this point in his testimony—is the incredible difficulty of minimization.

One doesn't have to have the kind of—I was going to say healthy, but maybe it is unhealthy—distrust of police listening to conclude that in good faith one has to hear an awful lot in order to decide whether one has a conspiracy of one kind or another.

And I think that has a chilling effect on all kinds of speech.

For example, let's take one really very troubling problem, to stick with this for a moment, where I will move beyond the First Amendment just for a moment, but it is related.

Mr. Nadjari and the other corruption investigators who use wiretapping pose very troubling problems for people like me—particularly Mr. Nadjari—not because of him and not because of the way he does things, but simply the nature of his task.

He is going after crooked judges—

PROFESSOR BLAKEY: And lawyers.

PROFESSOR SCHWARTZ: And lawyers, but essentially he is going after the judicial lawyers. But your interjection of 'crooked lawyers' means you see the point I am getting at, lawyer-client conversations, judge-lawyer conversations, judge-law clerk conversations, and a whole range of things that are really very hallowed in our constitutional hierarchy, and have been.

And that is a very serious problem, to know there is some guy around who is going after the judges in my community. And so when I call the judge or I call a client about something before that judge, then that means I am under surveillance.

Take, for example, the rather unhappy situation with one of the ablest judges in, I will say a depart-

ment that doesn't have many able judges, the Second District in Brooklyn. The State Supreme Court judges in Brooklyn are really not a terribly good bunch. I can say it openly because I assisted at one point in a lawsuit saying that publicly, the case of *Wallace v. Kern*. But there are a couple who are superb judges, like Judge Irwin Brownstein. And there was a report that one lawyer said to his client "I can get you Brownstein" on a case.

Well, apart from the impropriety of disclosing that kind of thing, which of course is a serious ethical matter, if they were concerned about Brownstein—well, the truth is I have one case with Judge Brownstein now. And I have spoken to him. The other lawyer has spoken to him. The two of us have spoken to him on the phone about various aspects. I have spoken with my client about this case I have with Judge Brownstein and it is an attempt to strike down the statute that prevents life-sentence prisoners from getting married. And I don't think there is much corruption in that. Certainly there is no money in that particular case.

But, nevertheless, that has a chilling effect.

And I don't think you can separate it out and say, "If we stay away from the New Left and if we stay away from Women's Strike and if we stay away from feminist organizations like NOW," then really there is no case for legitimate concern.

I think that is a distinction that is just not drawable, and I think in practice will not be drawable, because it seems to me if wiretapping is to be used anywhere, if organized crime does present a serious problem to our community—and I have some doubts as to whether it is responsible for everything from housemaid's knee to the common cold as has sometimes been indicated in various documents of one kind or another. In so far as it does—and of course it does—one of its major impacts is obviously corruption and what that does to a system of justice, with judges for sale, lawyers for sale, prosecutors for sale, cops for sale.

And even if wiretapping were more useful to corruption than some of these people say it is, we may pay a very, very heavy price.

CHAIRMAN ERICKSON: May I interrupt at this point?

It is just about the noon hour.

[Discussion off the record.]

CHAIRMAN ERICKSON: Let's recess at this point until 12:45.

[Whereupon, at 12:00 n., a luncheon recess was taken until 12:45 p.m.]

AFTERNOON SESSION

CHAIRMAN ERICKSON: Professor Blakey has yielded, with the thought that I might ask a few

questions, and then he would continue. The reason for doing that is, as you know, we are all tied up with airline schedules to some extent, and I did at least want to get your thoughts on various matters.

In so far as the report of the Administrative Office of the United States Courts is concerned, do you feel that the form of the report and the materials contained in the report at the present is such that it is performing the function that it was intended to perform?

PROFESSOR SCHWARTZ: At the risk of seeming to give a long answer, let me preface my response with an expression of appreciation to Mr. Blakey, because I am quite sure that that provision in the statute was a direct result of his efforts, as well as the establishment of this Commission.

I think we have too few of such things. And so my immediate answer is I am grateful for anything in this area, as in so many areas, where there is such a paucity of information.

Of course it can be made better.

I have not been terribly conscious of inadequacies in the reporting form.

CHAIRMAN ERICKSON: Don't you think it has gaps in it?

PROFESSOR SCHWARTZ: It does. I think, for example, one of the proposals in General Hodson's letter about sentences would be terribly useful to have. I think there is no question that the question of costs is really a wild kind of thing. I tried to make an analysis of the reports through 1971 or '72, as you will see in that ACLU report, and I found that with the state stuff, if it is a ball park figure it is an awfully big ball park.

With respect to such things as incriminating conversations, obviously that is a very subjective judgment.

I think that there is an assumption which the Administrative Office does not sufficiently dispel, that the arrests and convictions that are reported are a result of the installations involved. I think that should be dispelled.

Indeed, I found, curiously once, a prosecutor from Arizona wrote in 'We got one conviction, but it had nothing to do with the tap.'

I guess apart from that I really don't have too many complaints. It is a funny kind of thing, I have worked with the reports. I have cursed at them. I have tried to computerize them about four years ago and I found that the classification system for offenses was almost whimsical; it was almost impossible to work with.

This one troubles me very much, but it may not be a problem that the Administrative Office can do very much about.

I called them once and said, "How do you decide whether something is a gambling tap or this tap or that?" And he listed for me the priority of offenses and how they determined that.

It seemed to me that this was not a terribly good way of doing it, and I am not sure I know of a better way. But that I found very troubling.

I have made a suggestion, for example, that where the conviction takes place in the same year as the installation—or the arrest takes place in the same year as the installation—that the Administrative Office indicate for what offense the arrest or conviction was, because you can't know that from the way it is now. With respect to the supplementary reports, you can know, because they say so. So you can match up the original installation and find out what it was put in for and find out what they got. You can't do that when it happens the same year.

It is not too serious a problem because normally you don't get convictions the same year. You may get some. But the bulk of the convictions I find come in the second or third years.

You get the bulk of your arrests the first year, with just 20 per cent or so the second year and virtually nothing the third year. And, to follow up a comment I made a few minutes ago, with respect to Mr. Nadjari, he has gotten very few arrests associated with these installations.

CHAIRMAN ERICKSON: It may be that the regulations regarding the reports should be changed to make it possible to cause this report to have some meaning.

PROFESSOR SCHWARTZ: It is possible. I noticed Professor Lapidus noted—I have seen these reports myself in outline form, not in actual report—that there was an effort to ask them to assess the value of the installation. And I don't think that could do too much harm if taken with a sufficient grain or two of salt.

I think the real problem here is that for many of these problems only the kind of in-depth qualitative analysis that this Commission has actually embarked upon will give a complete picture.

My studies, I think—and I have a fair amount of confidence in them now; not so much the first year, but I do now—try to focus as much as possible on hard statistical correlations.

So I think those are the kinds of things that can be improved.

And I think with the computer thing, particularly, there is a certain freedom-of-information aspect of that so they will allow us outsiders to play with the computer and find out things that are in there. They will allow that. I notice they are unhappy with that.

CHAIRMAN ERICKSON: Are you concerned about the means for enforcing compliance?

PROFESSOR SCHWARTZ: That is a very serious problem. Again I am not sure how much you can do. I think the suggestion that you made this morning that they can't use it if they don't comply, is a little too Draconian. I can't see anybody buying that.

I am sure it will surprise you to hear me say that.

CHAIRMAN ERICKSON: With your candor, Professor, I don't think there is any surprise in any answer, because I know that regardless of what your views are you are going to give us your best judgment.

PROFESSOR SCHWARTZ: Thank you.

CHAIRMAN ERICKSON: The question I have is where do you draw the line? If it is Draconian to say you can't use the wiretapping procedure if you don't report, what other sanction would you give them?

PROFESSOR SCHWARTZ: I have an initial problem. The first problem is: How serious is the problem? How bad is the reporting, not in terms of sloppiness, about which you can't do much, but in terms of actual non-reporting? Because I don't know how much more you can do with sanctions. If the complaint is that they don't do a good job in reporting costs, if the complaint is that they are too subjective on what is incriminating—if there are things like that, I think that is almost impossible to enforce.

But if the complaint is that they are not reporting at all, that they are not filing the supplementaries—

CHAIRMAN ERICKSON: They are filing a skeletal report.

PROFESSOR SCHWARTZ: I don't know if this makes any sense at all, but it may be possible to impose fines, like the tax return, you know, if you don't file or file improperly.

CHAIRMAN ERICKSON: In the state courts?

PROFESSOR SCHWARTZ: Oh, the state courts. Is the state court a problem? Do they provide you with that kind of information?

CHAIRMAN ERICKSON: Well, the regulation requires that the judge—

PROFESSOR SCHWARTZ: I realize that. My impression when I look at the studies is that my problems are not with the court side of it. My problem is with the prosecutor side of it. Because the court side tends to be fairly formal: How many days did you authorize it for? How long was it in? What were the crimes? Who was the guy who asked for it?

I think there are about 8 or 10 items which I have found are generally adequately reported.

CHAIRMAN ERICKSON: Do you feel it would be too harsh to say that if, say, the prosecutor didn't properly report, that he couldn't again use wiretapping until he did complete the report?

Does that seem harsh?

PROFESSOR SCHWARTZ: No, no, especially since it is purely prospective rather than a penalty.

CHAIRMAN ERICKSON: Yes. How could you do anything more reasonable than that?

PROFESSOR SCHWARTZ: Well, I certainly wouldn't oppose something like that, and it might well do it.

CHAIRMAN ERICKSON: The reason I asked that was because it seemed a more practical approach than the fine.

PROFESSOR SCHWARTZ: I think it is a more practical approach. I threw the fine out and as I did I thought to myself, "You've got to be crazy." That is just not the kind of thing that works.

Your suggestion may be a viable kind of thing.

Again I have to ask: What exactly is the problem? Because it is my impression that with occasional "not reported," which are really relatively infrequent given the 700 or 800 reports that are filed, the real problem is sort of the feeling that "They've got to be kidding that this thing costs \$2,500 for ten days tapping" or things like that, where it is clear the reporting is simply filling in some number or that kind of thing. It is more a question of accuracy which is very hard to nail down.

Unless I am wrong about that, I would be interested in knowing from the Commission what the problems have been.

CHAIRMAN ERICKSON: I was going through these reports and find many have blanks or dashes where there is supposed to be information.

PROFESSOR SCHWARTZ: I have the impression that the dashes—I have noticed those primarily in the arrests and convictions and I have the feeling that that is where there is nothing to report.

CHAIRMAN ERICKSON: I was hopeful that we might get some recommendations as to ways that this could be improved. But I am certain that is going to take study.

PROFESSOR SCHWARTZ: I would certainly be happy to try to give it more thought than I have, and I must confess that I have not.

CHAIRMAN ERICKSON: Would you be willing to submit to us your thoughts on this?

PROFESSOR SCHWARTZ: Yes. As I say, I have some. Let me think some more.

CHAIRMAN ERICKSON: We would appreciate that.

PROFESSOR SCHWARTZ: What I haven't tried to do is, while working with these figures I haven't noted down "What do we do about this because it is so sloppy?"

I have just said, "Oh, for God's sake, I had better take into account this is a messy thing" and go on to other things. I will try to become more self-conscious about this.

CHAIRMAN ERICKSON: One of the other areas relates to this question of limiting the right of the state courts to utilize electronic surveillance procedures.

PROFESSOR SCHWARTZ: Yes.

CHAIRMAN ERICKSON: That would in essence, if we followed the suggestion that you made in that regard, force any area that involved electronic surveillance into the Federal courts.

PROFESSOR SCHWARTZ: Well, it would do more than that. My suggestion, if that is what you are referring to, would restrict it not just to the Federal courts but to the Federal prosecutor.

CHAIRMAN ERICKSON: Yes.

PROFESSOR SCHWARTZ: In other words, state prosecutors would not be permitted to do this thing and that is precisely what I suggested.

CHAIRMAN ERICKSON: You think the states ought to be deprived of this investigative tool?

PROFESSOR SCHWARTZ: Well, I think both the Federal and the state governments ought to be deprived of the investigative tool, but I think that a far worse case is made for state usage, especially since, as I think I indicated either in a private conversation or in testimony this morning, you cannot limit this to the one or two state authorities in whose judgment and usage you may have some confidence.

This is, in effect, an open sesame to the kind of thing that the Bronx District Attorney has expressed concern about, and to all kinds of abuses. As I understood the concern of the drafters and as I understood the point of the legislation, it was to get at organized crime, this cancer that was eating away at the innards of society.

And if that is the case, you just don't find much once you get outside of New York County—and there are a great many of us who don't think that Mr. Hogan has really done a hell of a good job in that area as well. And if he has, then I would say one has to look to the Organized Crime Task Force's comments back in 1967 that Los Angeles and Chicago have also done fairly well from time to time.

So that I have no hesitation in saying that if the purpose is to fight organized crime, and if we are dealing with a very dangerous instrument, the only place to allow use of that instrument is in the Federal prosecutors.

CHAIRMAN ERICKSON: Supposing we were to make the recommendation that states be governed by something that would be akin to the Federal

statute where the application would have to be approved by the Attorney General of that state?

PROFESSOR SCHWARTZ: Oh, I don't think that would make any difference.

CHAIRMAN ERICKSON: Do you think that would be an improvement?

PROFESSOR SCHWARTZ: Oh, yes, but a marginal improvement of no particular significance.

One has to start with the proposition, from my point of view—if you are asking me from that perspective—start from the proposition that wiretapping is a terrible thing to do to a society. And I echo what Ramsey Clark said yesterday, although not his eloquence.

And if you start with that proposition, then if you are going to allow it at all, you try to restrict it to those areas where it is absolutely indispensable. And from everything I have understood, the whole point of the Gambling Act, the point of the Organized Crime Control Act of 1970, the enormous expansion of Federal jurisdiction in this area over what are essentially local matters in Section 1955, is all premised on the notion that the states are not doing the job.

And if that is true, then it seems to me that undercuts the premises under which you allow state wiretapping.

And then when you add to it the fact that you can't really restrict it to the few cases, that if you give it to the Rackets Bureau in New York City you have to give it to the District Attorney in Des Moines, Iowa, if he wants it and can convince his state legislature, who testified before a committee "I would like to have wiretapping authority." They said to him, "Do you have an organized crime problem?" And I thought he was going to tell us about the giant octopus invading Des Moines and he said, "Oh no, but it would be nice to have."

It seems to me in making social policy one has to assume you will never get the optimum. The slip-page, the wastage, the screw-ups and the misfirings and the unintended consequences always are terribly significant.

And it seems to me before you go around playing with fire like this—and of course it all assumes my judgment that you are playing with fire when you are dealing with wiretapping—before you do you start it on a very limited basis. And that is the basis for my hostility to allowing it on the state level.

CHAIRMAN ERICKSON: I think that we would agree on the fact that the bug, the electronic bug, is a far greater invasion than the wiretap.

PROFESSOR SCHWARTZ: Yes, we would.

CHAIRMAN ERICKSON: And should there be a different measure for using a bug than for using a wiretap?

PROFESSOR SCHWARTZ: Well, my position has been that bugging should be outlawed altogether. I am talking about the third-party bug, not the consensual bug.

CHAIRMAN ERICKSON: No, I am talking about the bug that is used in connection with the telephone, where it is actually acting as a transmitter, if you will, and picking up every sound in the room.

PROFESSOR SCHWARTZ: Yes, even when the telephone isn't used.

CHAIRMAN ERICKSON: Yes.

PROFESSOR SCHWARTZ: I know. That is what I am talking about.

CHAIRMAN ERICKSON: All right.

PROFESSOR SCHWARTZ: And in my piece for the Trial Lawyer Association I discussed some of the history, that when wiretap legislation was first proposed, the Justice Department opposed a bill by, I think it was, Senator Keating when he was then a Congressman to allow bugging. And they opposed it on the ground that it raised very complex constitutional and privacy considerations which hadn't been thought through.

I don't know that those have ever been thought through. The distinction that was in fact drawn by the Kennedy Justice Department at that time was completely obliterated in Title III, and it seems to me that for the very same reasons that I think the Justice Department originally was dubious, I would not allow it.

There is a follow-up question which may be the one that you had in mind, which is: All right, suppose you did allow it. Would you require a different set of conditions?

CHAIRMAN ERICKSON: That's it.

PROFESSOR SCHWARTZ: That, I think, is the precise question but I am as guilty of long preambles to answering questions as anybody else.

I think as to that I really find it so troubling that I really don't want to answer it. I think the room bug is one of the most troubling things modern technology has devised. There is no way to make it comply with the Fourth Amendment except on one situation, and that is the situation which, curiously, is the only one that has come before the Supreme Court. And this came up in the *Goldman* case, for example, where you have almost a staged meeting by a group of conspirators.

What happened in the *Goldman* case is that a government informant who knew about a bankruptcy fraud scheme—it was some kind of commercial fraud scheme; I think it was bankruptcy—told the FBI about this and the FBI said to the informant, "Set up a meeting at such and such a time and we will bug the meeting." And the bug was in place only during that meeting.

But that is not the way it is going to be used. That is the only time in my judgment that it could comply with the Fourth Amendment, but it seems to me that is not going to happen. It is not going to be used only that way. And I just think it should not be allowed, period.

I can see a telephone tap—in fact, I have changed my mind, Mr Blakey will probably be happy to know. I can see occasions where the Fourth Amendment can be complied with in telephone tapping, and it is essentially the *Katz* case.

PROFESSOR BLAKEY: Would the reporter please italicize that part.

[Laughter.]

CHAIRMAN ERICKSON: You see the reason for my question is that following your line of thinking, if we are going to say there should be a differentiation between the two, that can be accomplished in various ways:

One, by providing the additional requirements for using a bug.

PROFESSOR SCHWARTZ: Yes.

CHAIRMAN ERICKSON: Or by limiting the provisions of Title III merely to wiretapping.

PROFESSOR SCHWARTZ: That is certainly the way my line of thinking is going. Obviously, anybody involved in the practical world of trying to get better legislation knows that the best is often the enemy of the better, and I would be happy with any improvement in that area.

But it seems to me the problem with writing the statute and the problem of real limitation—I guess if I had to write a statute I would try to model it on the kind of factual pattern that you had in a case like *Goldman*, which means that it went on—and even in the *Katz* case, which was also actually a Detectaphone. It wasn't a telephone tap as you recall, but a bug on the phone booth which overheard one end of the conversation.

CHAIRMAN ERICKSON: And they were selective.

PROFESSOR SCHWARTZ: They were very selective. That is precisely the point. I would say there has to be knowledge pretty much of the conversation.

I disagree with Professor Lapidus on the notion you never know in advance what the conversation is. That is not true. Now the gambling conversation is a little different. I once tried to analyze out how one could improve the 'type of conversation' provision in the statute to make it somewhat more refined.

And gambling is complicated except I will say it is my impression most times a tap in a gambling case is to really get evidence of the interstate na-

ture of the operation. It isn't that hard, as Clark said yesterday, just to get information that there is a bookmaking operation going on.

CHAIRMAN ERICKSON: If we are looking at gambling, gambling is endemic to the telephone.

PROFESSOR SCHWARTZ: Yes. And by and large we are talking about an operation where at ten o'clock the phone starts operating, and from 10:00 to 3:00 there really isn't very much going on, frankly, besides I guess what horse or what game and how many points and that kind of stuff. But you don't use bugs for that.

I would think that once you get away from that you can start specifying. You tend to know in advance.

Looking at some of these cases where the wiretap was used—not gambling but what some of us would consider more serious offenses—you can know in advance what it is that you are trying to find out. You know who the parties are, or at least who some of them are likely to be. You know what the subject matter very often is. You know roughly what time it is going to be. And that can be specified.

And I would think that if you can't do that, then you are going on a fishing expedition, and if you are going on a fishing expedition, you don't do that consistent with the Fourth Amendment.

And I am just talking about Fourth Amendment. The First Amendment problem that Mr. Blakey adverts to obviously is one of these more general considerations which is virtually all or nothing. That is the nice thing about the Fourth Amendment, that you can write in balancing and regulatory devices to try to make a reasonable balance.

So I would think that if you are going to say something about bugging, I would hope you would not stop at that, but actually suggest that, for reasons back in 1961 that are just as good now, there is just no need for it; it is just too pernicious and dangerous and should be out. If you are going to make a change, I think it should be in terms of just the one conversation.

Let me add one more thing about the bug that just occurs to me. Many of the lawyer-client over-hearings are where there was a bug in a room.

CHAIRMAN ERICKSON: What was that?

PROFESSOR SCHWARTZ: Many of the lawyer-client conversations that were overheard are on room bugs where the lawyer comes in and they discuss things.

CHAIRMAN ERICKSON: I'm sure that is true.

PROFESSOR SCHWARTZ: Yes, sir.

CHAIRMAN ERICKSON: But the question we have in trying to review this entire matter is to try to make recommendations, if you will, not only to protect privacy but to fulfill the legitimate needs of

law enforcement, but in such a way that constitutional principles are not violated.

So I am trying to get your guidance to steer us around a few of these difficult areas.

PROFESSOR SCHWARTZ: Well, I gave you a clear path for your steering, which is no, none of this kind of bugging.

And in terms of the impact on law enforcement, I haven't checked out—perhaps the Commission will or has—the relative success of bugs as opposed to taps. If the success for bugs is not much different from that for taps, then the giving up of the relatively small number of bugs that are installed doesn't strike me as likely to strike much of a body blow against law enforcement.

CHAIRMAN ERICKSON: There is this difference. Yesterday we were talking about reasonable expectation of privacy.

PROFESSOR SCHWARTZ: Yes.

CHAIRMAN ERICKSON: When you talk over the phone I think you would agree, as a lawyer who has attended criminal cases, you don't speak with the freedom that you would speak if you were in your own office.

PROFESSOR SCHWARTZ: Alas, no.

CHAIRMAN ERICKSON: That is one of the recognitions. And if you were on a party line you would be less apt to talk than if you are on a private line; isn't that true?

PROFESSOR SCHWARTZ: Sure.

CHAIRMAN ERICKSON: So when it comes to wiretapping, that again is not as much of an invasion as the bug?

PROFESSOR SCHWARTZ: Oh, I agree with you.

CHAIRMAN ERICKSON: But the bug, for the same reason, if there is going to be criminal discourse, is more apt to pick up the information than the tap?

PROFESSOR SCHWARTZ: Well, my point on that is that I would like to see an analysis to determine whether or not that has in fact happened, whether the bug has been more productive than the tap.

My impression is—and it is only an impression; I haven't made these studies—that they use a bug when they think the information they are seeking is not going to be on a phone but is going to be in a room—not that that is a more productive way of doing it, but they are not going to get it on the phone; they are only going to get it in a room. And that means it is no more likely to produce valid results than the average tap. And for those reasons I don't know that there is much lost.

But I must confess—I think we are looking at this from different perspectives, because to me what is

to start with a very troubling instrument becomes immeasurably so when we are talking about a room bug. You don't have to use the phone. You've got to live somewhere. And there is no place to hide with a room bug. And that often involves the additional factor of break-in to a house—because very often there is no other way of getting into a place. You can't install the bug, like you can a tap, from outside.

And the experience with bugs is not good. There was the room bug in a bedroom for 15 months in the *Irvine* case. Police engaged in this kind of work think they are engaged in a rough and tumble business on both sides and aren't terribly finicky about what they do. I think they are not very finicky about a client's privilege. Police think a defendant's lawyer is almost as bad as the defendant himself.

So I don't notice any fastidiousness about not intruding on lawyer-client conversations. Indeed, I checked out a bunch of the cases which had made it to the Supreme Court in wiretapping and over and over again we find lawyer-client conversations involved.

CHAIRMAN ERICKSON: Beginning with *Coplon* and then going on back, the lawyer-client area, which is a Sixth Amendment right and we even talked about it, earlier this morning, the bugging of the conversation between lawyer and client in a jail—

PROFESSOR SCHWARTZ: Sure.

CHAIRMAN ERICKSON: —that is uniformly stricken and condemned.

PROFESSOR SCHWARTZ: Sure, but that is just law. All that says is that they are not supposed to do it.

CHAIRMAN ERICKSON: I think at the time these things occur the courts have been outraged in their condemnation of the conduct. They never suggested it be pursued.

PROFESSOR SCHWARTZ: I never suggested that. All I am talking about is what you can't discover in the way of these intrusions.

I can tell you I have tried in several of our cases—and it is not just my own experience—to find out whether there is wiretapping in a case and when you do find out, you find out not very much.

CHAIRMAN ERICKSON: It is a long road.

PROFESSOR SCHWARTZ: In the *Weathermen* case in Detroit, a mass of logs was turned over in a domestic security case. And in the course of that a lot of things were left out.

By accident a bunch of logs were turned over, and through those they were able to find out about more tapes. And listening to the additional tapes, they found innumerable lawyer-client conversations that they never knew about except through this ac-

cident of the FBI having mistakenly turned over some documents that they weren't supposed to.

CHAIRMAN ERICKSON: You recall in the *Alderman* case it was on a petition for rehearing after certiorari had been denied that the Solicitor General made the disclosure that there had been a bug and there had been electronic eavesdropping, but he had examined those transcripts and had found nothing that would fall within the *Brady v. Maryland* exception, and therefore there was no reason to turn it over.

And of course in the ultimate case—

PROFESSOR SCHWARTZ: —the Supreme Court went the other way.

CHAIRMAN ERICKSON: They went the other way.

So the point I am getting at is to say that I think perhaps this goes into another area that we have to deal with as far as the prosecutors are concerned. The code of professional responsibility is a great step above the old canons of professional ethics.

PROFESSOR SCHWARTZ: Yes, it is.

CHAIRMAN ERICKSON: But maybe amendments are required to cover this.

As you know, Colorado and several other states have put in very strong ethics opinions dealing with the lawyer who transcribes the telephone conversation with a fellow lawyer without disclosing the fact that he has taken down the conversation on an electronic device.

PROFESSOR SCHWARTZ: I think in all fairness, Mr Chairman, my concern here is not with the lawyer. My concern is with the person who is doing the listening. And I couldn't agree more with what both Mr. Clark and Mr. Andersen said yesterday about how the investigator, the policeman, the FBI agent doesn't tell the lawyer everything. What we have in our criminal justice system, as I am sure you know far better than I, is this series of sub-systems which co-exist uneasily with each other.

And I will never forget in 1960 or '61 when I first got interested in the whole wiretap question I went to a New York Bar Association dinner, and there was a member of the New York United States Attorney's staff there and he was talking off the record. We asked him about wiretapping. And he said, 'Look, I don't know anything about wiretapping and I don't want to know anything about wiretapping. What the FBI agent tells me about information he obtains, I don't ask too much because if it turns out it is in wiretapping, it will jeopardize my case.'

And that is what it is. It is a 'hear no evil, see no evil' attitude on the part of the prosecutors. Where you are dealing with illicit activity on the part of the investigator, it is understood and I don't anticipate changing something so fundamental.

PROFESSOR BLAKEY: Professor, do you think it is fair to characterize all prosecutors and all policemen that way?

PROFESSOR SCHWARTZ: No, and I haven't characterized them all. But I am worried about enough of them to think it is a serious problem.

CHAIRMAN ERICKSON: The American Bar Association in promulgating the standards of criminal justice—and some of us on this Commission have some passing familiarity with that—have really made inroads into this problem you have talked about. The *Brady v. Maryland* matter is dealt with, and discovery and procedure before trial standards; the prosecutor and defense function, the electronic surveillance standards—

PROFESSOR SCHWARTZ: I have less approbation for that.

CHAIRMAN ERICKSON: And any violation of these is called unprofessional conduct. I was inquiring whether further amendments to the Code of Professional Responsibility were dictated, or have you given that any thought?

PROFESSOR SCHWARTZ: I haven't given it any extended thought. I just have a couple of reactions to what you are saying now.

And I think what I am saying is that the kinds of things you are worried about, namely intrusion on Sixth Amendment rights, the kind of thing—I suppose you were instrumental in that Colorado opinion on ethical questions on surveillance by a lawyer—those kind of things I think are presently covered. I don't think there is any question that no lawyer who values his oath at all and his duty as an officer of the court, would ever knowingly intrude on another lawyer's conversations with his clients.

But what I am saying is that just like the free press-fair trial standards, they go only to the lawyers.

As I recall the free press-fair trial standards, they say nothing about the police chief and the detective making statements.

CHAIRMAN ERICKSON: The standards recommended that in the police function standards.

PROFESSOR SCHWARTZ: Yes, but you can't discipline the police chief, whereas you can with a lawyer.

CHAIRMAN ERICKSON: These are all problems that of course I think fall somewhat beyond the limits of this Commission.

PROFESSOR SCHWARTZ: Yes.

CHAIRMAN ERICKSON: But they are problems that we are aware of and are trying to deal with.

PROFESSOR SCHWARTZ: What I am saying is that the problems I am concerned about are the problems that are referred to in the Bronx report and elsewhere, which is that it is not the lawyer

who is the problem in many of these cases; it is the policeman, the investigator, over whom there is very little control, except that it is a crime if he does something wrong. And that is just a meaningless control. I can't recall anybody having been prosecuted.

CHAIRMAN ERICKSON: Now let's take the next step.

When we have illegal use of wiretapping or electronic surveillance, I think the two of us again would be in agreement in saying there should be vigorous enforcement of that right. And I think the testimony developed by Congressman Kastenmeier who is a member of this Commission, and the information he developed through our staff's work relating to some local police being involved in illegal surveillance and no enforcement by the FBI, would bring about the need to consider how we are going to enforce the provisions of the statute if there is illegal wiretapping.

What would be your thoughts on the way it should be enforced? Should there be a special prosecutor that does nothing but review these reports and pursue the illegal sales, the illegal use of electronic surveillance? How should it be done?

PROFESSOR SCHWARTZ: I don't know the answer to that. The notion of a special prosecutor for this is an attractive one except for the fact that we will soon have a special prosecutor for everything under the sun. And I am not sure that there is a lot of confidence—

CHAIRMAN ERICKSON: There have been a limited number of prosecutions.

PROFESSOR SCHWARTZ: I know, very well.

The problem is, it seems to me, that there are two kinds of illegal wiretapping on the part of police.

There is, first, the kind that everybody would say is illegal. They are wiretapping because they want a share of the take, because they are engaged in law enforcement; they are corrupt all the way.

As to that, I don't know the reasons for the non-enforcement. My guess is they simply haven't been able to catch them.

The second kind of illegal surveillance, the overzealous kind, the kind that engages in sample tapping, the kind that doesn't abide by the rules, the kind that taps illegally because they don't have enough to get a warrant, or something like that—no FBI is going to go against those people. The FBI depends on these people. There are close working relationships as we all know between the Bureau and local police. We read this morning in the paper about close cooperation between the CIA and the Washington police.

CHAIRMAN ERICKSON: That is why I asked you how to do it.

PROFESSOR SCHWARTZ: I think you can't do it. I think you ought to abolish this statute because I think a statute like this brings along with it a whole train of troubles, and that you can't—when you are dealing with essentially a diseased enterprise, patching here and there is just giving aspirin for a cancer. I think the wiretap statute produces these things.

CHAIRMAN ERICKSON: Now, we know that narcotics has been on the scene and we have the Drug Enforcement Administration.

PROFESSOR SCHWARTZ: Yes.

CHAIRMAN ERICKSON: Should there be an electronic enforcement administration to carry out the prosecution of any of these illegal sales? And I don't think anyone questions the fact that you can buy any kind of bug you want without difficulty.

PROFESSOR SCHWARTZ: Well, that is a slightly different matter, Mr. Chairman.

Of course, no one will question that fact. There was a program on Mike Wallace's '60 Minutes' on precisely that, ten blocks from the Department of Justice.

CHAIRMAN ERICKSON: I am saying if we are going to create something like this it ought to cover the whole thing.

PROFESSOR SCHWARTZ: I guess my problem there is really primarily one of ignorance, and I can't really help you.

The reason for the ignorance is I don't know why those cases aren't prosecuted. I haven't looked into it. I haven't spoken to the Justice Department. Wallace went to see this guy in the Justice Department on television and said, 'I just bought this. Why don't you do something about it and don't you know something about it?' and the man said, 'Oh, I didn't know it.'

Obviously, that was nonsense. Everybody knew it.

PROFESSOR BLAKEY: Just for the record I am aware that the FBI, on more than one occasion, has investigated the shop to which we all periodically refer. It would seem that that shop advertises more than it sells. Efforts to make—and I won't indicate now which agency was involved—to make an 'undercover buy' from it turned up equipment that could not be fairly described as designed for surreptitious surveillance.

PROFESSOR SCHWARTZ: Then that is, in a way, a partial answer to the question that I have raised, which is: What is the problem? The partial answer there is in a way that the received wisdom isn't that wise; isn't that correct?

Again, I have to know a good deal more.

I do know, for example, that prior to Title III it was said by people in the Department that they

couldn't enforce Section 605 because they couldn't prove this interception divulgence.

Mr. Kastenmeier thereupon put in a bill which would eliminate the requirement for proof of divulgence and said, 'Now go out and this will do your job for you.'

I'm sorry, but I confess I cannot give you an answer because I don't know enough.

CHAIRMAN ERICKSON: You think there is room for some improvement in that area?

PROFESSOR SCHWARTZ: It is my impression there is room for a great deal of improvement.

I know the *Wall Street Journal* did a story on it once because they called me and I gave them the same answer as I gave you, 'I don't know much about it.'

Part of the problem, of course, may be technological. But it is my impression that an awful lot of stuff that is used for electronic surveillance also has quite innocent uses. And if that is the case, then you may be fighting an impossible battle, because—

CHAIRMAN ERICKSON: Let me make one thing clear. I am certain that there has been investigation of these complaints. It is a difficult area.

PROFESSOR SCHWARTZ: Yes.

CHAIRMAN ERICKSON: And I am trying to suggest that there is a way of improving this. There is a means of keeping the FBI from having to turn in its big brother that they have to work with on every case. I think that is an insurmountable burden to put on them in some of these cases, and I was asking whether or not this procedure that I outlined might have some effect.

PROFESSOR SCHWARTZ: Let me suggest something to come back to, an older theme of mine and a more fundamental theme.

I heard testimony this morning—I think it was this morning—that part of the reason this stuff is on the market is because those that are sold to policemen ultimately work their way into the private market one way or another. And that kind of supports a thesis which I have expressed many times already today, which is that when you loose this kind of stuff into society, you cannot limit it very effectively.

CHAIRMAN ERICKSON: All right.

PROFESSOR SCHWARTZ: And therefore there shouldn't be electronic equipment in the hands of the police and there shouldn't be electronic equipment in the hands of other law enforcement agencies, and then you will not have no problem on these matters, but you will have a good deal less.

CHAIRMAN ERICKSON: I suggest there might be an area for licensing the manufacturers. Then it would be possible to trace the item.

And of course it seems to have been a rather effective enforcement tool when it came to sub-machine guns and sawed-off shotguns and things like that.

PROFESSOR SCHWARTZ: Has it been effective in the area of shotguns? I don't know about sub-machine guns but I don't know that shotguns, sawed-off or otherwise, are hard to come by.

CHAIRMAN ERICKSON: They are not bought and sold in the open market. You can't go down to the sporting goods store and buy a sawed-off shotgun.

PROFESSOR SCHWARTZ: All I can say is I am just not of much help in that regard.

CHAIRMAN ERICKSON: You don't know whether licensing would be of value or not, or can you give an opinion?

PROFESSOR SCHWARTZ: I can't give an opinion.

CHAIRMAN ERICKSON: You are aware that the Canadian Act has one of the 'harmless air' provisions?

PROFESSOR SCHWARTZ: I think, as I testified earlier today, I am not aware of what is in the Canadian Act. I only know there is legislation which is modeled somewhat on ours.

CHAIRMAN ERICKSON: As far as judge-shopping, which is one of the complaints, don't you feel a seizure such as Judge Stern set forward yesterday avoids—

PROFESSOR SCHWARTZ: I think so. I think that is one of the things something can be done about. The statute simply says, as I recall, 'to judge of competent jurisdiction'—it is really much too loose.

And I have collected in one of the things I did examples of what seemed to me rather gross judge-shopping, although I am told some of that—

CHAIRMAN ERICKSON: Professor, you know your criticism of New Jersey is occasioned by the fact that the judges up there were designated by the Chief Judge and therefore you didn't have shopping.

PROFESSOR SCHWARTZ: That is what I understand.

CHAIRMAN ERICKSON: And therefore your criticism that it all went to the same judges was a statement of the provision in the New Jersey statute that prohibited that.

PROFESSOR SCHWARTZ: I know about that.

CHAIRMAN ERICKSON: I just thought I'd get an admission in the record.

PROFESSOR SCHWARTZ: If you want to find admissions of error, I have even noted an admission of error of \$40 in my prepared statement.

I know about that. However, I know about Buf-falo where there isn't anything like that and one or two judges have gotten the overwhelming bulk of this.

I know this is true elsewhere and it seems to me this is the kind of thing—

CHAIRMAN ERICKSON: That is remediable, there is no question about that. And I am not sure the New Jersey experience would be such that it would be subject to criticism.

In regard to tapping for strategic intelligence, do you feel that could be permitted under any statutory authority that would meet constitutional muster?

PROFESSOR SCHWARTZ: No.

CHAIRMAN ERICKSON: Would your experience with wiretapping be such that you would have the opinion that the information gained from either taps or bugs generally provides intelligence material, but not admissible evidence?

PROFESSOR SCHWARTZ: Could that question be read back?

CHAIRMAN ERICKSON: I will restate it just to save a moment.

In your experience with wiretapping and electronic surveillance, would it be your opinion that the information developed from those two sources primarily produces strategic intelligence information and not direct evidence of a crime?

PROFESSOR SCHWARTZ: I see now what troubled me about the question. And I had some problems with your exchange with Professor Lapidus this morning about that, also.

I think there are not two categories of evidence that we are talking about, but three categories: Direct evidence of crime, indirect evidence of crime, and the strategic intelligence, which, as I understand it, isn't necessarily linked to any crime at all but gives you general information about 'the enemy'—organization, structure, mode of operation, associations, and the like.

And consequently, the thrust of your questions earlier today about direct and indirect evidence of crime—I have trouble with.

To answer your question, if I may rephrase it the way I did, the direct and indirect evidence of crime being, to use Mr. Blakey's phrase, tactical intelligence geared to a specific crime or crimes, as opposed to strategic intelligence when you are going after a person and want to know all about that person.

I think that the success—it is hard to know how to evaluate this, what is success and what isn't.

This is enormously difficult in crime and other things. It is my impression, on the basis of the data in your report, that electronic surveillance is relatively successful—and I indicated in my report what

those figures amount to roughly—in drug cases. It is very expensive for some reason in drug cases, but relatively successful, at least on the Federal level.

It is somewhat less successful in gambling cases. And I am talking here about evidence of crime, the tactical intelligence.

As to the—to use a word that was used yesterday in rather extended exchange between Mr. Blakey and Mr. Clark—productivity, the productiveness of the taps with respect to strategic intelligence, it is my impression that one learns a fair amount about the activities of certain people who are under suspicion.

How to balance these relatively, I really can't say.

My information in my study, for example, indicated that for the 1969 through 1972 Federal taps, approximately 137 out of 395 were in some way associated with a gambling conviction; that 21 out of 56 were in some way associated with a drug conviction of some kind.

I use the word 'drug' rather than 'narcotics' because it includes marijuana which is not a narcotic and it includes cocaine which is not a narcotic.

With respect to other kinds of things, it is 13 out of 35.

I can't say whether the taps prior to 1969, which is the only time when I think constitutionally the Federal Government has engaged in strategic intelligence taps—I cannot say whether those were more successful or less than these taps.

I would say, by the way—and I don't mean to get into a debate about which I know absolutely nothing, but just listening to your exchange with Mr. Clark yesterday on that Cary Parker report, I would guess the basic difference between you was that Mr. Clark was looking to what those produced in the way of convictions. And according to the hundred or so decisions, those judges found there was no link in all but three.

PROFESSOR BLAKEY: If that is what he meant, he really should have made it clear in his book.

PROFESSOR SCHWARTZ: He said—

PROFESSOR BLAKEY: Let me comment on that because that is one of the central differences between us.

You can see from the context in which the statement was made: he testified before the Canadian Parliament, and the issue before them was whether to adopt a court-ordered system. And they wondered if it was useful in obtaining evidence of crime. His testimony was that this kind of equipment used in these ways is not productive of information that can be produced in court. And he cited Carey Parker's position in support of that.

If he means that the pre-1965 surveillance produced no convictions, you can agree with him.

But can you adopt a court-ordered system that will make taps that will give you information?

You know, as I know, that the Organized Crime Task Force report of the President's Crime Commission reached the conclusion that only the FBI had been able to develop a picture of the national structure of La Cosa Nostra. And that information was obtained through this strategic intelligence bugging program.

PROFESSOR SCHWARTZ: Yes, but I think that is nonsense. I think the picture of the organized crime task force was a bill of goods that was sold to the American people, that Donald Cressey put together in a paper that most say is based on a tissue of speculations. And the notion of this nationwide syndicate—the report in Chicago or somewhere else refers to a loose confederation at most in the city.

So if that is what we learned, I would say we didn't learn much that was reliable. And I would also add, which is the other thing I wanted to say, that it was also Clark's point yesterday—and I knew I made a mistake in raising this—that we didn't learn much that we didn't know before. The Valachi testimony told us a great deal about what happened in 1931 and we didn't learn much that would help us in prosecuting cases because, if it did, we might have caught some of these people and prosecuted them in 1967 and '68 which we haven't done.

There was a story by Nicholas Gage last year which said we haven't made a dent in organized crime, whatever it is or whoever it is.

And so it seems to me I agree with Mr. Clark.

CHAIRMAN ERICKSON: Well, you have now zeroed in on an area that I was going to concentrate on and that is: What is organized crime?

PROFESSOR SCHWARTZ: That is for Mr. Blakey and what I call the organized criminologists to say.

I don't purport to be an expert in this at all. Whatever organized crime is, Mr. Blakey and other people in the Organized Crime Section know far more about it than I do.

CHAIRMAN ERICKSON: Would you agree that there is at least, this loose confederation—that might be tighter than loose in the viewpoint of some—that is nationwide? Certainly the gambling operation is tied together nationwide.

PROFESSOR SCHWARTZ: Well, again, I am not talking about something that I feel very confident talking about. I don't have an impression that the gambling operation is nationwide. I have a feeling that there are a lot of nationwide gambling operations.

And as Adam Smith said years ago in the *Wealth of Nations*, 'When people of the same persuasion and the same calling come together, they talk business.' And I assume that when they come together, they talk business.

But this is a far cry from the mighty empire against whom you are bidden to wage a war. This is a far cry from the kind of thing that we have to bend all of our resources to.

I do not agree that organized crime is the number one problem of our community, as Robert Kennedy apparently thought it was, in his early years—not later.

CHAIRMAN ERICKSON: Here is what I mean—

PROFESSOR SCHWARTZ: Let me add one final thing. I don't get the impression our seven years of wiretapping under Title III or the many years prior to Title III have made much of a dent in it.

CHAIRMAN ERICKSON: Well, in connection with the enactment of legislation to combat what was either a real or a spectre of an evil that faces our country, various interstate crime acts were enacted. And these interstate acts have been subjects of various prosecutions. So there is some indication of interstate activity.

PROFESSOR SCHWARTZ: Well, indication of interstate activity is a far cry from the notion of a massive operation.

CHAIRMAN ERICKSON: I understand that.

PROFESSOR SCHWARTZ: But let me go further and say I am not saying that organized crime is a spectre. What I am saying is that I don't have the impression from my reading and some study in the matter that it is quite the octopus that is cracked up to be.

I know in my own city I was told by defense lawyers about the syndicate who get a share of every big burglary—not by name but that there are people who are involved, and in many other ways.

I have been reading some material in a book that will soon come out—not soon, but will come out in a year or so—by Charles Silberman—who did *Crisis in Black and White*—in which he talks about organized crime, the fencing, the corruption of the government, and that kind of thing in the world of street crime, and how these things are interlocked and the importance of that.

I don't mean to minimize the fact that we have a problem, and a real problem, and a problem that involves corruption, involves a whole range of other things.

But that is different from what we find—

CHAIRMAN ERICKSON: I understand your point, but going to the next thing that comes right down the line: If the law of conspiracy is

there—and conspiracies are not hatched in the light of day, but are put together in the dark of night in a hidden place—in order to combat such conspiracies, there does have to be something other than physical surveillance and there has to be more than the plain tools that the policeman of yesterday used; isn't that true?

PROFESSOR SCHWARTZ: Yes.

CHAIRMAN ERICKSON: And isn't one means of obtaining evidence relating to a conspiracy to bug?

PROFESSOR SCHWARTZ: Yes. I have never said that isn't the means of obtaining evidence. What I am saying is that it is a two-way—

CHAIRMAN ERICKSON: That it is too great a price to pay?

PROFESSOR SCHWARTZ: It is too great a price to pay even if we got a great deal from it and there is no indication that we get that.

I mean the way I have tried to put it, I guess, is that Professor Lapidus this morning was not right when she said, "This is the age-old problem between liberty and security." I don't think there is that kind of problem here because wiretapping doesn't give us very much security.

CHAIRMAN ERICKSON: Do you believe if we are to go forward permitting wiretapping, that to insure that, say, the emergency provision that is now in the Act, but hasn't been used, is not followed, that some procedure such as that that they use in Arizona and California, where they provide for an electronic or telephonic authorization for a search warrant might be a reason for putting such a provision in any statute that might be enacted to improve this procedure?

PROFESSOR SCHWARTZ: Yes, I think in my exchange with Mr. Blakey I gave that this morning, Yes, I think it would

CHAIRMAN ERICKSON: You don't have any quarrel with the fact that if a judge is called and the information given him over the phone and it was recorded and transcribed within 48 hours that would give as much protection as we have now under the present procedures?

PROFESSOR SCHWARTZ: I think so. I think so. The important thing, I think, is two-fold. One is to introduce the neutral magistrate for whatever good that does, but secondly, I think perhaps an even more important thing is to make sure that you have a contemporaneous statement of what it was that the police relied upon.

CHAIRMAN ERICKSON: Now, that leads me to the last area that I will burden you with, and I do want to thank you—

PROFESSOR SCHWARTZ: It is a very pleasant burden.

CHAIRMAN ERICKSON: —for being of great assistance in this area.

And that goes to the consensual tapping.

I understand your concern about consensual tapping. But isn't it far better to have a conversation set in concrete where it is not my version as contrasted to his that is being outlined before the jury for their determination, particularly when you have, say, an informant involved who is offering information but has no reliability?

PROFESSOR SCHWARTZ: Well, I have two answers to that, if I may give them.

The first is that the recording often isn't that accurate. It misses a great deal very often. Those things just don't work that well, particularly if it is a transmitter.

CHAIRMAN ERICKSON: But assuming we've gotten by that mechanical difficulty.

PROFESSOR SCHWARTZ: I may be drummed out of the corps. I may depart from Mr. Clark on this because I think he took a position of opposition to this.

I don't oppose consensual surveillance in the absolute terms that I do third-party surveillance.

What I have suggested in this area, with various refinements depending on the circumstances, is that it be done pursuant to a warrant.

I think the problem is really a problem not so much of electronic surveillance and intrusion of privacy of the kind that we have in the third-party surveillance, but essentially a problem of betrayal. And it is a problem which really, if one is to talk in terms of shorthand case law, is a problem that involves *Hoffa*, where there was no electronic surveillance, and the *White* case, of course. And there is a great deal of hard logic, difficult logic to spin away from, in Justice White's statement for—it wasn't a majority, but a plurality of four in the *White* case—that it is hard to distinguish between the human bug and the electronic bug.

I thought Justice Harlan made a very moving statement, and I am not at all sure that the average person one asked wouldn't react in his gut with a comment, "Oh, yes, it is different if there is a wire," but would be hard put to analyze out why the difference.

The basic problem in this area is that police seem to rely on and need informants. I see that as rather different from wiretapping—not consensual wiretapping, but third-party wiretapping.

CHAIRMAN ERICKSON: As far as use of informants by police, that is essential.

PROFESSOR SCHWARTZ: That is my impression.

CHAIRMAN ERICKSON: Because of the fact that we are not dealing with the Rover Boys, we are dealing with—

PROFESSOR SCHWARTZ: I am not disputing that. That is precisely my point.

CHAIRMAN ERICKSON: Right. And these informants are not always the most truthful individuals.

PROFESSOR SCHWARTZ: That is right.

CHAIRMAN ERICKSON: So, for the purpose of solidifying what the informant says, if you have a bug on him and he consents to it, it is the only way you can tell that he is telling the truth?

PROFESSOR SCHWARTZ: That is right. And I am suggesting that when you have that kind of situation it ought to be done when you have probable cause and ought to be done pursuant to a court order.

And I see this—and my thinking is admittedly kind of sloppy on this—as one way of trying to bring the use of informers under some kind of control.

I am not calling, as I am with third-party surveillance, for abolition. I am calling for some kind of control.

And maybe here—I hesitate to say this—taking up the invitation of Justice Powell in *U.S. v. U.S. District Court* and these other cases, that maybe a different kind of supervisory judicial control could be imposed here.

I notice this morning you suggested the possibility of perhaps approval from the Attorney General, the top prosecutor in this area. I think I heard that.

CHAIRMAN ERICKSON: Yes.

PROFESSOR SCHWARTZ: Instead of a judicial authorization. And it may be that that would be a good step forward for use of this kind of thing—of consensual surveillance—perhaps with a statute writing in some criteria as to when he is to grant that approval, rather than saying, 'It shall be done on his approval whenever he feels like it,' which would transfer the locus of arbitrary power from the police to the prosecutor.

So I think that would be a step forward in this area.

CHAIRMAN ERICKSON: Now you, as I understand it, are not pleased with the *Rathbun* exception?

PROFESSOR SCHWARTZ: Well, *Rathbun* really is a kind of complicated case, because it is not a pure consensual surveillance. It involves—it is not clear whether it was because of the consent factor, which is the way it has been interpreted—and I have a feeling probably correctly, but I am not sure—or because it was the use of an extension phone and that somehow was not considered within the statutory meaning of 'intercept.'

CHAIRMAN ERICKSON: I understand that and, of course, Title III—

PROFESSOR SCHWARTZ: My displeasure with the *Rathbun* case—and I don't recall having expressed that much displeasure—is that it leaves this kind of thing completely uncontrolled.

For example, it is said that after all if I speak to an informer he might tell somebody else, and what difference does it make whether there is a wire or something like that; in effect, the problem is one of betrayal.

I don't think that is quite true if the consent is obtained, as it so often is, either by a deal or by pressure of some kind or other. At that point it really becomes a search, a surreptitious search. And it is not simply that I talk to you and you decide you are going to turn on me. It is a different thing. It is a search of my things. It is an interrogation of me. I don't want to raise the *Massiah* case, although it went up as a Fourth Amendment case.

I think once you are dealing with that kind of situation the notion of reasonable expectation of privacy is really not that far-fetched. The notion is that I have an expectation that the cops are not going to send somebody in to inveigle himself into my confidence and then probe.

I give as a standard example to students now the *Hoffa* case, only with certain variations. And the variations are that the informer is somebody whom the suspect does not know in advance. The informer inveigles himself and cajoles his way in.

And I think that makes a difference. I don't think it would make a difference with today's Supreme Court—

CHAIRMAN ERICKSON: With the entrapment case of the last term—

PROFESSOR SCHWARTZ: I agree with you on that, but I am not talking about entrapment in the legal sense. I am simply talking about creating evidence. And I am saying this kind of probe is quite close to a Fourth Amendment search, directed toward one's thoughts. It is not very much different, in my opinion, from someone breaking in and stealing. Because I don't know that inveigling your way in and trapping somebody into talking—in the entrapment—by saying 'I am an old buddy' is a search. And I think in that context there ought to be some kind of judicial control so it is not done on hunch.

Because I think betrayal, use of informers, is a terribly pernicious thing in a free society. I have seen its impact in my own life, in the Attica case where it was disclosed that a young woman named Mary Jo Cook was an FBI informer.

I have seen the impact on the community in which she lived; the defense teams with which she was associated, including my own in the Attica case. I know the people she lived with, had roman-

tic relations with. And I think this is a terrible thing to happen in a free society.

CHAIRMAN ERICKSON: There is no question about it, the informer is not the most popular person, and his longevity, once his identity becomes known, is such that insurability is gone.

But as far as the facts of life and crime are concerned, the informer is with us and always will be.

PROFESSOR SCHWARTZ: I agree with that. What I am saying is that it ought to be brought under some control.

CHAIRMAN ERICKSON: I appreciate your putting up with me this long, Professor.

Now you will be granted the opportunity to have Professor Blakey review with you the thoughts that he has on this subject that the two of you probably have captured as the experts in the field.

PROFESSOR SCHWARTZ: I think what you are really saying is you are now going to turn me over to the tender mercies of Professor Blakey.

CHAIRMAN ERICKSON: Thank you.

We will take a five-minute recess.

[Whereupon, a short recess was taken.]

PROFESSOR BLAKEY: Professor, are you familiar with the Fifth Circuit case of *Simpson v. Simpson*?

PROFESSOR SCHWARTZ: Somewhat familiar with it. I think I have seen a report of it in the *Criminal Law Reporter*, the excerpt.

PROFESSOR BLAKEY: This is the one where a husband conducted a wiretap on a wife, and obtained some information on the wife's paramour. The husband played transcripts to neighbors and the wife's attorney, based on which the attorney recommended a consent divorce.

PROFESSOR SCHWARTZ: Yes, I am familiar with it.

PROFESSOR BLAKEY: Subsequently, the wife sued the husband for illegal wiretapping, and the Fifth Circuit ruled that since it was in her family, being husband and wife, and inside the house, and no third party was involved in the surveillance itself, despite the language of the statute, because of the legislative history, they denied a right of recovery.

I wonder if you'd comment on the implications of that from its privacy aspect?

PROFESSOR SCHWARTZ: I find the decision, as you have described it—and your description fits my recollection quite precisely—quite impossible to understand. I thought we had sort of come past that time of the world when husband and wife were one, especially when they were close to each other.

PROFESSOR BLAKEY: One, and the one was the husband.

PROFESSOR SCHWARTZ: And the one was the husband.

PROFESSOR BLAKEY: And I can't see how they could have read that position into the statute. There is an old joke about, 'When the statute is clear, turn to the legislative history.'

They seem to have taken the joke literally.

PROFESSOR SCHWARTZ: That is right. And it seems to me that it is just not consistent with the statute.

You were instrumental in drafting the statute, and I don't know how much one ever has a right to go back to the guy who is responsible for it in terms of drafting and so on, but I'd be interested in your own reaction.

PROFESSOR BLAKEY: One of the problems that bothered me is that when they got to the legislative history, they said the only indication in the legislative history contrary to their position was a statement by Professor Blakey in the House hearings that it might have covered this sort of situation.

PROFESSOR SCHWARTZ: And that didn't count.

PROFESSOR BLAKEY: And that wasn't enough.

Frankly, I had thought in reading—and I don't want to testify myself—but in your own reading of the legislative history, did you construe the enormous debate on police use to limit the comprehensive nature of the provisions?

PROFESSOR SCHWARTZ: No. Indeed, it seemed to me one of the major arguments in favor of the legislation by its proponents was that it would, indeed, offer greater protection of privacy. And there were no distinctions drawn between husband-wife situations and other situations. I take it that they would have come to the same ridiculous conclusion if the husband had hired a private detective.

PROFESSOR BLAKEY: No, they said if he had it would have been illegal.

PROFESSOR SCHWARTZ: That is ridiculous, because the detective is serving, if not as a common-law agent, as a representative. And we have known for many years—you probably know more than I about this—that one of the major abuses or, if you will, not abuses but actually illegalities in the area of wiretapping was precisely in the area of husband-wife relations—husband-wife and business relationships. Those were the two gross areas.

PROFESSOR BLAKEY: Did you have any doubt in your mind that the legislative history clearly covered both of those areas to the maximum degree permitted by federalism considerations, under the commerce clause?

PROFESSOR SCHWARTZ: I have no doubt. I didn't think precisely about that, but if somebody

had asked me after I studied the legislative history on the floor of the House and Senate and the discussion, and the ABA report which was the forerunner of that, I would have said, of course, it is covered. If that isn't covered, what sort of private surveillance is? Because that is one of the most common forms.

PROFESSOR BLAKEY: It is also one of the most vicious invasions of privacy, not business secrets but literally the intimacies of personal relations.

PROFESSOR SCHWARTZ: I would agree with that. Indeed, I would go so far as to say that although I find the consent exception for private persons ambiguous—the references to, 'a private person cannot engage in consent surveillance if for a tortuous purpose or with an injurious intent,' I find that ambiguous—I would have thought that the kind of situation in the *Simon* case was precisely that covered by that consent situation, and that therefore, not only could you not do third-party surveillance but you couldn't do consent surveillance either. Because that is precisely what we talked about.

There is an additional factor. You are familiar, I'm sure, and the staff is, with a case in New York called *Applebaum*, which created an exception for wiretapping by the subscriber. I don't know where I got the impression—from the legislative history or somewhere else—that the statute was not intended to incorporate the *Applebaum* rule.

PROFESSOR BLAKEY: My memory is not good enough to tell you now that *Applebaum* is quoted in the legislative history and explicitly rejected. I will tell you that the discussion on the staff level was that *Applebaum* was a bad case and should be overruled by the statute.

PROFESSOR SCHWARTZ: And it was overruled by the New York statute which preceded Title III.

PROFESSOR BLAKEY: Let me move on to consensuals. You will recall some of the discussion of Professor Uviller.

PROFESSOR SCHWARTZ: No, I can't because I wasn't here.

PROFESSOR BLAKEY: I tried to explore with him what kind of court orders you should obtain in this area. And the issue I initially raised with him was that you know, as I knew he knew, that search warrant practice, as it grew up in common law, was a kind of writ of replevin. Your stolen property was in someone's house, and because it was your property you could go in and get it out. Ideas surrounding judicial supervision of searches grew up in that context; they didn't deal with the supervision of police, but the regulation of property rights.

What this means is the framework of the Fourth Amendment and search warrant practice isn't always adapted to the supervision of police work.

And I think this comes sharply to the fore in consensual areas.

If what you are asking for is the principle of judicial review, it is very difficult to argue against that.

But I want to go further and explore with you: What would be the criteria of judicial review, and give you two examples.

The testimony in the record indicates the consensual transmitter is used typically not so much to gather evidence but to protect the officer. He is going into a narcotics buy. Narcotics buys are often violent situations. Sometimes the narcotics buy turns into a narcotics rip-off where the buy money is stolen. And to permit the undercover officer or special employee into a house or apartment house substantially risks his life.

Now, if you could show case by case the possibility of danger, I am sure a traditional search warrant with probable cause to indicate danger might adequately serve for a warrant.

However, the testimony in the record tends to indicate that what we would have in this area is not case-by-case showing of danger, but rather class showing of danger.

You know the problem with no-knock in New York, *Delago*, as against the California case, which said you had to show the possibility of the destruction of evidence, not in gambling cases generally or narcotics cases generally, but tied to this buy or tied to this raid.

If this kind of 'tied to this raid' rule were applied in this danger area, it seems to me a significant number of officers would be forced to go in to buys not equipped with Kel transmitters, and thus unprotected.

PROFESSOR SCHWARTZ: There is a question at the end of that?

PROFESSOR BLAKEY: No, the question mark comes next: Do you think—as a public policy question now—because we are not talking about constitutional law any more—we can develop standards for consensuals in this area that make class judgments rather than individual judgments?

PROFESSOR SCHWARTZ: The way you set up the hypothetical, I don't think so. Because it seems to me that within the framework of a situation such as you have describe, it would be very easy to develop a traditional warrant. Namely, when someone goes in to make a buy, in effect he is going in to obtain evidence, I take it with probable cause—or not. If not, maybe he shouldn't be allowed to do that.

And I think the specificity problems, which in a way are what you are dealing with, might well be appropriate.

I do think, and I will say, and I am sad to say, that there is clearly a form of constitutional authority for your class warrant kind of situation. I find that a very troubling authority, but it's there, and that is the string of cases from *Camara against Municipal Court* all the way through *Almelda Sanchez* and Powell's concurrence, which allows that kind of class warrant.

They tend to rely in both cases on somewhat more objective criteria than the kind you are talking about, which is danger. In other words, they rely in *Almelda Sanchez* on some things that you can handle with numbers, and so on.

But I would be very loathe to adopt that unless it were shown to me that a more conventional kind of warrant, geared to a specific buy and a specific situation, created very serious problems.

PROFESSOR BLAKEY: What troubles me is the interests involved here are not simply gathering evidence versus privacy, but the safety of the officer.

PROFESSOR SCHWARTZ: Oh, I agree with that.

PROFESSOR BLAKEY: Versus the privacy of the citizen.

PROFESSOR SCHWARTZ: Yes.

PROFESSOR BLAKEY: And if you take the 'stop and frisk' cases as your guide, the safety of the officer sometimes balances more importantly than the privacy of the citizen.

PROFESSOR SCHWARTZ: But you are raising a different consideration, a consideration that may be at least as important. But what you are saying is that, in the first place, there is this danger. Okay—but maybe not.

In the second place, you have got to do something about it—clearly okay.

What do we do in the 'stop and frisk' case? We try to, as the court said in *Terry*, look for some specific objective thing, some specific objective, I guess indication—to use Rehnquist's words—'indicia of danger.' We ask for a specific showing.

I don't know whether that is true in practice or not, and maybe what they really said was, 'Whenever you have suspicion of armed robbery, you've got it'—maybe. But the fact is there was still some kind of precise and specific showing of that.

So in effect what you are doing is you are saying, 'Insofar as that specific indication of need is concerned, we are not going to insist on it.'

And I don't have the impression that we need to dispense with that.

Let me say that it is my impression, talking to policemen and reading the cases—and it is only based on that; believe it or not I was a prosecutor, unlike Mr. Clark, at one point, but I didn't have the wiretap—not for very long.

But it isn't my impression that someone is wired very early in the game. It is my impression that the wire goes on when they are pretty much ready to go, and they zero in on somebody when they are ready to make the buy, when they are ready to wrap up the matter.

I know, for example, in the Leslie Fiedler case in Buffalo, she was wired several times, particularly when the buy was made.

By the way, I do think that was a long question.

PROFESSOR BLAKEY: That's all right. There is another follow-up. There is a second leg to it.

In those situations where you had probable cause in traditional sense to secure the evidence, I take it your point is that you could wire him for the evidence purpose, and the danger point would be served, too.

PROFESSOR SCHWARTZ: Yes, yes.

PROFESSOR BLAKEY: Let me take you down to the second leg. As I said, that may not always be true, but my impression is it is usually not.

I will give you an example where it is not true. Let me raise this one with you.

The other typical use that is made of the one-party consent is for verification purposes. It is the *Osborn* bug, where Vick, the informant, comes in. Vick is not known to be reliable, and the information that he gives you is incredible on its face, that Tommy Osborn, a leading member of the Tennessee Bar, is corrupt.

Now, you could not swear before the judge, 'This man is credible and I have reason to believe his information.'

You wire him and send him in to verify his information.

Under traditional probable cause standards, which meant you could expect Tommy Osborn to give information, you could not have gotten the *Osborn* bug if you were going to apply traditional probable cause standards.

PROFESSOR SCHWARTZ: I don't read *Osborn* that way. I think they had probable cause. I think Vick went to the two judges and said, 'This is what is happening. This is how I know.'

He was an ex-policeman, after all, who was working for Walter Sheridan. He wasn't an anonymous informant.

I would have thought under *Spinelli* and *Aguilar* and *Harris* and that whole line, you did have probable cause in that case.

PROFESSOR BLAKEY: The feeling of the attorneys involved, whom I know, is that if the judge had turned to them and said, 'Do you believe Vick,' they would have said no.

In other words, they did not feel they had probable cause. The reason they went in with the consensual was to obtain probable cause and verification.

PROFESSOR SCHWARTZ: Well, I would say if that is the only problem with that—and I haven't thought about this, but off the top of my head I would say that if the only problem is that you have an unreliable informant or an informant you can't meet the reliability standard for and that is why you are doing it, but you have everything else, I would think that kind of warrant would certainly satisfy me, especially since as a practical matter the court has been steadily eroding the reliability requirement. A case like *Harris v. United States* doesn't leave too much.

PROFESSOR BLAKEY: This is particularly important in one dimension of consensuials. We have had testimony from James Thompson of Illinois that probably most are used to obtain information, not to inculcate, but used to obtain information to exculpate. The guy gives you a story; you don't believe him, and you are in a dilemma. If you put the man on trial based on testimony you don't believe in, you ruin a man; you may get a wrongful conviction. The thing to do at that point is to send him in for verification in order hopefully to exculpate.

PROFESSOR SCHWARTZ: As I think through that on the spot, and unaccustomed as I am to three or four hours of public grilling—as I think about it, that kind of situation doesn't bother me. The reason it doesn't is because it seems to me the single most important aspect of the probable cause requirement is not the subsidiary questions involved in *Spinelli* and *Aguilar*, but really when you add it all up, is there a basis whereby the community is justified in doing something to somebody?

And here I think the consensual surveillance is less of an intrusion than the third-party surveillance. And if the only problem is that the reliability problem of *Aguilar* or *Spinelli* is not met but you have a police officer or prosecutor, and you have a story, which if believed constitutes probable cause, then I don't think I'd have a problem with that.

Now, maybe I will give myself an escape hatch and say if you ever blame that on me and I think about it some more, I won't deny it but say I did it off the top of my head.

PROFESSOR BLAKEY: This is a three-legged stool. Let me ask you the third question.

PROFESSOR SCHWARTZ: That is probably where it will fall.

PROFESSOR BLAKEY: Do you recognize the general emergency notion, the hot pursuit notion?

If there is no time to get to the court, would you permit the person to be wired and go in anyway?

Let me tell you why I raise this.

PROFESSOR SCHWARTZ: I am trying to think of what situations this would arise in. Maybe you can help me with that.

PROFESSOR BLAKEY: The Department of Justice has given us statistics indicating since January of 1969 they have used consensual surveillance other than phone in approximately 5,000 cases, 50 per cent of which were utilized under emergency conditions.

PROFESSOR SCHWARTZ: What is 'emergency'?

PROFESSOR BLAKEY: An emergency condition is no time to obtain the Attorney General's permission.

PROFESSOR SCHWARTZ: My question about it is: What will be lost? In other words, normally I think as a practical matter the exigent circumstances situation in a conventional search tends to deal with destruction of evidence. That is the usual thing. The safety to life is really a fairly minor aspect—it is the destruction of evidence. That was certainly true in *Hayder v. Warden*, and it has been true in the other cases.

What is the emergency in this kind of situation where you are really not so much talking about destruction of evidence as you are talking about a form of surreptitious interrogation?

PROFESSOR BLAKEY: I will give you an example.

PROFESSOR SCHWARTZ: That's what I want.

PROFESSOR BLAKEY: The Lopez-type situation, where an IRS agent goes in to engage in conversation—

PROFESSOR SCHWARTZ: Yes.

PROFESSOR BLAKEY: That is not what I mean.

PROFESSOR SCHWARTZ: Yes.

PROFESSOR BLAKEY: What I have in mind is the kind of situation where a bribery is going to occur. There is going to be a meet in which it is going to be discussed.

PROFESSOR SCHWARTZ: What did you say?

PROFESSOR BLAKEY: A bribery meeting. Or a loan shark is meeting a man in a hotel to collect the debt, and the loan shark has set up the meeting. And the victim comes to you and says, 'What can you do for me?' And there really is no time to do anything but wire the man up. And you wire him up, first to protect him so you can intervene in time if they are going to beat him, but second, for incontrovertible evidence of extortion.

This is not uncommon.

PROFESSOR SCHWARTZ: I guess I have a couple of responses to that.

The first response is pure expediency. Anything is better than we have now so I will throw out something with exceptions.

The second response is—I am always good at exceptions—where there are a lot of searches.

So I find that troubling.

I guess my third limitation really has to do with the fact that I have a lot of trouble seeing what the emergency is.

There are two parts to the warrant, as I have said many times today. The first is to take the decision-making power as to the search away from the exclusive control of the police.

The second is to make a record of what the police were acting on so later at a suppression hearing you know what information they really had.

I would think with the second one there is no problem about emergency. All it takes is just sitting down dictating into a machine, into a sealed machine.

I would think also that if it happens during the day, again surely there is a half-hour, an hour, an hour-and-a-half leeway when one can find a commissioner or a magistrate. Judges really don't hesitate for hours and don't reserve decision so that the argument takes place in January, and the decision is in June or the following year or two later.

I really have the feeling—and I am imputing somewhat bad faith—that because of the volume of what is involved—5,000 is a fair number. What we are talking about is, from what you tell me, from 750 to 1,000 a year, and if we throw in the states where there may be even more, we are talking about a lot of work and a lot of paper work.

I am not persuaded by the arguments as stated. And from what I know about dealing with judges—I know, for example, in the Leslie Fiedler case, I know in the Martin Schlosberg case the warrant was obtained at 11:00 o'clock at night. And the warrant was obtained from a judge who was on duty, and they went to him.

PROFESSOR BLAKEY: Let me move on—

PROFESSOR SCHWARTZ: Let me add one final thing. If no judge is available, I think one could write in something, either regulatory or some kind of a form, that if no judge is available they make the record and go, but if a judge is available they have to go to him.

PROFESSOR BLAKEY: Let me change the subject slightly and raise with you some general questions about the character of the analysis that you have made, the cost-benefit analysis, and ask you first initially a very broad question.

Do you think statistics are really the measure of justice?

And put it this way: Traditionally, we have said such things as, "Better that nine innocent go free than one guilty be convicted." We have really tried to look at justice as an individual matter not only for freeing innocent people. A large number of people expressed great concern when we had civil rights violations in the South. But it wasn't a large statistical number of civil rights violations. It was the fact that we thought it was important that it occurred.

Do you think we can fairly evaluate cost-benefit effectiveness by simply adding up figures?

PROFESSOR SCHWARTZ: Well, in the first place, I don't think this can be said to be simply adding up figures. Whoever—I take it it was you—put the provision in for reports and for data, the notion was that knowledge was relevant and could help, and that it was knowledge relating to inevitable numbers of people called and numbers of people overheard, and amount of money, and that kind of thing.

The fact is that I think statistics are terribly relevant. The problem is I don't know how good the statistics are.

PROFESSOR BLAKEY: But—

PROFESSOR SCHWARTZ: Let me finish. Because it seems to be one of the major concerns here, if we are going to decide this question of social policy: What does it cost the community?

And it costs the community in lots of ways. It costs the community in loss of privacy. It costs the community in dollars. It costs the community in diversion of mental resources. It costs the community in terms of what kinds of things we think worth focusing on, because there is an opportunity cost here, because if we focus on this, the odds are that public attention will not go to that.

It also costs the community when we have crime. It also costs the community in dollars and cents—a whole range of ways.

One of the factors has to do with the kind of information that is, in fact, provided by statistical data.

PROFESSOR BLAKEY: Would you agree with me that is one factor? I see in your own materials you criticized the gambling cases because they got little fellows, not big fellows.

PROFESSOR SCHWARTZ: Yes.

PROFESSOR BLAKEY: And I take it you feel if wiretapping had got big fellows then, well maybe catching one big fellow is more important than catching five little ones, although it is five to one if we quantify.

PROFESSOR SCHWARTZ: No, what I have said in dealing precisely with that issue in the 1973 report that I have is that those things are very, very

difficult. How do we analyze the numbers that we have? What does it mean to say that 100, 200, 500 people were convicted?

Well, by a process of elimination, it means nothing to say 500, 200, 100 were convicted if the ultimate purpose of the statute, which is, as I understand it, to make a meaningful dent in organized crime, is not furthered.

PROFESSOR BLAKEY: In other words, the statistics at the beginning of the analysis. We must look beyond quantity to quality.

PROFESSOR SCHWARTZ: That is what I have tried to do. But it also seems to me that if the statistics aren't very significant, if we don't have very big numbers, then an even heavier burden is on the proponents to say that those numbers that we have are big numbers individually.

PROFESSOR BLAKEY: Let me move on to the next, I guess, very difficult question in evaluating need.

How can we really evaluate need in this area?

I'm trying to raise that question with you. Let me give you a long question and give you an opportunity for a long answer.

PROFESSOR SCHWARTZ: I will try for a short answer.

PROFESSOR BLAKEY: In a scientific study in a laboratory you can take measurements and you publish your scientific study. Anyone else can replicate the measurements. Anyone can check it out.

In social science studies, you can get a large enough pool of materials, to add, subtract, multiply, and divide.

The great difficulty here is that it looks like we are comparing apples and oranges. How do you compare the effectiveness of Hogan's office in Manhattan against Dan Ward's office in Chicago. Dan Ward didn't have it and said it wasn't necessary. Frank Hogan had it and said it was necessary.

Do you think in the realistic future—this is the question—we will ever be able to come up with empirical data to establish usefulness that will have the kind of hardness that we can find in the scientific laboratory?

PROFESSOR SCHWARTZ: Yes and no. The "no" part is that it is very likely that we will not match scientific studies, whatever they are, although my friends in the chemistry and other faculties tell me that social scientists, humanists—call it what you will—grossly exaggerate the hardness of the physical scientific data, particularly when you move into more advanced unknowns, where the design of the experiment becomes terribly important to the outcome.

The "yes" part of it, however, is that we can estimate what the results are of various efforts, if Hogan's office claims they got 15 members of organized crime in 15 prosecutions and sent them away for an average of two years each.

And if Dan Ward's office, to take an unrealistic example, says, "We got 50 and sent them away for 10 years," and both offices seem to agree that the people are of the same relative importance, we have some idea.

You are absolutely right that in matters of social policy we tend to fly by the seat of our pants, and then you know the famous phrase from Cardozo, "The engineers do things better with logarithms." They do, but that is not what social policy is about.

PROFESSOR BLAKEY: But—

PROFESSOR SCHWARTZ: Let me finish. Because it seems to me if we can make comparisons, the organized crime force made those judgements about relative effectiveness, and it seems to me we can.

And, of course, I wind up with the proposition that if we can't—and here is the fundamental difference between us, I think, and something I think is worth saying.

The fundamental difference between us is that if we cannot decide, then I think the burden is on you because we have invaded privacy. And I think, therefore, you lost.

In your judgment it may well be that you feel that law enforcement and that side of it is so important that that burden is more on me, in which case I lose.

PROFESSOR BLAKEY: What may well be is that we both have to recognize that we cannot find adequate empirical data and that we have to more or less fly by the seat of our pants and make the kinds of expert judgments based on all the evidence we have. Isn't that what we all have to do?

PROFESSOR SCHWARTZ: Yes, but we have evidence as to convictions; we have evidence as to arrests. If a guy comes in and says, "As a result of 50 taps I picked up a bunch of bookies who got a \$100 fine each," or "\$200 fine each," I don't think you have to be a James Coleman or an Eric Erickson or one of the great sociologists of our time, or anything else, to conclude that, "Gee, wiretapping can't be terribly useful if they just don't wind up with anything."

PROFESSOR BLAKEY: All right.

PROFESSOR SCHWARTZ: And it seems to me in my judgment that is the kind of evidence we come close to having.

PROFESSOR BLAKEY: Let me carry this further.

Certainly to a degree we are going to have to make our evaluation based on expert opinion such as your own or the opinion of others who have testified, people who have clinical data as opposed to empirical data. Wouldn't you agree?

PROFESSOR SCHWARTZ: I assume that in this judgment that you are going to make and that I have been trying to make, clinical judgment of the kind that you have had before you and that I have looked at to some extent, and this kind of statistical data, will be explored.

Let me say, however, that a lot of it has to be evaluated with respect to source and interest.

PROFESSOR BLAKEY: Let's kind of go down—which is my next question. You seemingly are answering my questions before I can ask them.

What are some of the criteria we ought to apply in evaluating these things? Should we look at past experience? If he has worked with wiretapping?

PROFESSOR SCHWARTZ: Yes.

PROFESSOR BLAKEY: Should we look to see what kind of success he has had in his office, whatever success means?

PROFESSOR SCHWARTZ: Yes.

PROFESSOR BLAKEY: Should we look at the kind of problem he has? For example, a North Dakota prosecutor who comes in and says, "I have had wiretapping, and I have been very successful; I have licked my crime problem," ought not be placed on the same scale as a district attorney from Manhattan. If we are going to match up a district attorney from Manhattan with a district attorney from L.A.—

PROFESSOR SCHWARTZ: I have seen statements from district attorneys of Manhattan and L.A., and I assume that is a factor.

PROFESSOR BLAKEY: Everyone can have an opinion but not every opinion is worth having.

PROFESSOR SCHWARTZ: On the risk of walking into a trap, I'll say I agree with that.

PROFESSOR BLAKEY: Believe me, Professor, I wouldn't attempt to set you up.

PROFESSOR SCHWARTZ: It has been my experience—a slight digression—that the worst witnesses in the world are lawyers. They talk too much.

PROFESSOR BLAKEY: I suspect that for interrogators it is the same.

Let me raise another question with you, and again it is a kind of philosophical one. Sometimes when I am sitting at home thinking about these problems and trying to evaluate them: Should we have *Miranda*? Shouldn't we have *Miranda*? Should we have wiretapping or shouldn't we have wiretapping?

What bothers me is it is something like a theater of the absurd. As I see the problem with the organized crime situation, there is really only one problem in the criminal justice area—volume. In other words, the system is in a state of virtual collapse, processing cases that literally spill out of the police department and into the prosecutors office. Discussions about sophisticated issues, such as wiretapping and trying to compare the experience of an office like Manhattan with an office like that in the Bronx, when both offices—and I don't mean to criticize either office—are in a state of virtual collapse because of volume, is almost to engage in an absurdity.

Can we really talk about fine-tuning of a system that is today, because of volume of crime, absence of resources, in a state of virtual collapse?

PROFESSOR SCHWARTZ: I must confess it seems to me that I don't see the drift of the question. I agree with that so completely. I agree completely with the notion that volume, sheer bodies and inadequate resources, is perhaps the central problem of the criminal justice system of our country. We are incredibly niggardly about that aspect of it. And it seems to me that one just has to walk into an ordinary criminal court and not look for anything, and that problem just explodes in front of your eyes, overworked this, that, and everybody else.

But it seems to me the implication for the inability to engage in fine tuning means that this incredibly, to me, dangerous instrument, the proper use of which depends upon fine tuning—that that instrument should not be used because you are not going to get that fine tuning. And that is precisely one of the points that I have tried to make, somewhat ad nauseam, I think, which is that it is impossible under the best of circumstances to have a wiretap system which is not going to be abused, which doesn't harm people, which doesn't do, by my prejudices, predilections, whatever it is that led to my conclusions, including study of the reports—that is not going to do a hell of a lot more harm than good.

PROFESSOR BLAKEY: You may find this as somewhat of a surprise, but I don't really disagree with what you said.

If the system cannot handle it, it ought not have it, and it may well be that as long as we are understaffed, undermanned, undertrained, and inundated with general crime, it may be silly to give them wiretapping. They won't be able to use it effectively anyway.

PROFESSOR SCHWARTZ: I happen to agree with precisely that conclusion for some of the reasons you have stated.

And I think, not to narrow your point but I think it must be said, that problem is especially acute on the state level.

PROFESSOR BLAKEY: And in the major metropolitan areas.

PROFESSOR SCHWARTZ: Yes, which is where the major wiretap authority is sought.

PROFESSOR BLAKEY: And at the local levels.

PROFESSOR SCHWARTZ: So what I guess I am saying, therefore, is that I think the implications cut across all jurisdictions. But I think it is especially true on the state level, if we are to draw a distinction between the state and Federal thing, which it seemed to me the original Kennedy bill pointed to, but obviously for political reasons could not do.

PROFESSOR BLAKEY: You suggested earlier to the Chairman that we cut out the states. Aren't you troubled by the possible implications of having wiretapping done only by the Federal people?

PROFESSOR SCHWARTZ: You'd better elaborate what those implications are and then I will decide.

PROFESSOR BLAKEY: One of the things people constantly worry about is a police state. In other words, an abusive national administration is an abusive administration of 200 million people, whereas abusive administration of one county is that county only, or of one state is that state only.

It may be a good argument to say, "Let's eliminate it on the Federal level and only permit it at the state level, not the local level."

PROFESSOR SCHWARTZ: No, I don't face those implications. And the reason I don't face those implications is because only one of the reasons for my objection to wiretapping has to do with the kind of abuses that result from such gross volumes.

As you know, I oppose this device on the Federal level for lots and lots of reasons. And I think that the implication of what I am saying is that it is especially bad at the state level. And I think the police state problem is there very much because of the existence of Federal wiretapping, and that problem—and for the reasons I have set out—points toward abolition at the Federal level as well—not necessarily, however, the problem of numbers. I may be wrong about the numbers at the Federal level but I don't think it's that kind of problem.

PROFESSOR BLAKEY: One of the issues you continually raise is alternatives to fighting organized crime with the criminal justice system.

You suggested the legalization of gambling, for example.

PROFESSOR SCHWARTZ: I have suggested that in the past with more assurance than I would

now. It is not so much that I have changed my mind, but I have done some reading lately which makes the issue a somewhat more problematic one.

PROFESSOR BLAKEY: Are you familiar with the Twentieth Century Fund study, "Easy Money?"

PROFESSOR SCHWARTZ: I am not familiar with the study. I know of the study. And it is because of that kind of thing that I—it is not that I have changed my mind about that because I really think gamblers should be decriminalized for other reasons, apart from the corruption and everything else. And that has to do with class justice.

When I was a young lawyer on Wall Street, or actually on Park Avenue, I engaged, and my colleagues did, in a great deal of gambling, except that we called it playing the stock market. We did not call it playing the numbers. We played a different kind of numbers game.

So there are a lot of such factors involved there.

I think with respect to gambling—I think I am for decriminalization, but in a forum like this, as opposed to cocktail parties, I would want to do some more reading and thinking about it.

PROFESSOR BLAKEY: The reason I raised it was I was involved in the Twentieth Century Fund study, and the kind of conclusions we came up with—either socialization, where the government runs it, or good old-fashioned laissez faire—are not too desirable. We came to the conclusion that decriminalization was not a substitute for a fight on organized crime and that organized crime has not been substantially hurt where decriminalization has occurred. Many of the things people seek in the illicit game presently would be sought even if it were decriminalized tomorrow.

PROFESSOR SCHWARTZ: Sure.

PROFESSOR BLAKEY: Tax evasion, confidentiality, things of that nature.

PROFESSOR SCHWARTZ: Yes.

PROFESSOR BLAKEY: So I am wondering if decriminalization as an alternative to fighting gambling through wiretapping is viable.

PROFESSOR SCHWARTZ: I think there are a couple of issues about it, and I'd rather put them in the form of questions or issues rather than assertions because I don't feel very sure of my ground here.

I would think part of the reason for that, assuming it to be the case, is that to some extent I wonder how much organized crime still is in gambling anyway.

Conventional organized crime, as some recent studies have indicated—you are probably familiar with Frank Iannis' "Black Mafia," and that sort of stuff. It is not in there. It is a dark area. It is something we don't know much about.

Secondly, it is also my impression that in the international narcotics trade organized crime is deeply involved. And it may well be that that is another factor, that in effect you cut off but one area of operations.

Thirdly, as I understand it—and here I would defer to almost anybody else's judgment—organized crime really lives off a lot of illicit services and things—not just gambling, not just prostitution, but a whole range of these things. And my guess is that decriminalizing one of them would do some good but would not be the whole answer.

PROFESSOR BLAKEY: Suppose we—

PROFESSOR SCHWARTZ: Let me just finish.

I happen to think—and again I would defer to others on this; I happen to think the narcotics question—

PROFESSOR BLAKEY: That's the next question.

PROFESSOR SCHWARTZ: In the narcotics area, I really believe in heroin maintenance. I think that we are, as others have said, a drug culture in many, many ways; that the heroin business is just going to be there.

PROFESSOR BLAKEY: Who would take the drugs? Would you describe for me the typical addict today?

PROFESSOR SCHWARTZ: I take it it would be the typical lower-class black person, just as I would guess that today the typical alcoholic is white. I take it that drugs—

PROFESSOR BLAKEY: What do you think would be the reaction of the black community if we undertook to initiate a heroin-maintenance program?

PROFESSOR SCHWARTZ: Oh, I have no doubt about that, and I am not here to win votes in the black community or any other community. The Rockefeller drug program, which I consider one of the most hypocritical pieces of barbarism—and I use those words only because I can't think of stronger words—was applauded by a fair number of people in the black community—I think wrong-headedly, but it was, because heroin is a serious problem.

But a lot of the problem has to do with the way that heroin is distributed, the corruption, the unsanitary aspects, what it does to have to hustle. In other words, it is the whole aura of the illegal heroin culture that at least contributes to the scourge that heroin is in a community.

PROFESSOR BLAKEY: What about the destruction of the personality of the user?

PROFESSOR SCHWARTZ: I don't know that is necessarily the case. Harry Anslinger boasted that

he was maintaining two Congressmen on heroin. I don't know whether they had destroyed personalities or not.

In England, which has a very different problem, of course—I don't want to match the two and, of course, they are having problems there—but in England, the mere fact of heroin maintenance does not mean that those people on maintenance are necessarily destroyed. They do live productive lives. Indeed, the evidence that I have is that heroin in and of itself has relatively little pharmacological or physical significance.

PROFESSOR BLAKEY: This is probably not the place to go fully into the heroin maintenance program.

PROFESSOR SCHWARTZ: Yes, and I am not the person to do it.

PROFESSOR BLAKEY: Would you grant me, as you yourself suggested previously, that decriminalization of heroin, like the decriminalization of gambling, poses a number of very sophisticated problems?

PROFESSOR SCHWARTZ: Yes.

PROFESSOR BLAKEY: And that people ought not respond in the fight against organized crime, "decriminalize gambling, decriminalize heroin; that's the easy way out." It is not the easy way out.

PROFESSOR SCHWARTZ: I agree.

PROFESSOR BLAKEY: The issues raised by these alternatives may be as significant as the issues raised by wiretapping itself.

PROFESSOR SCHWARTZ: Yes, but the problem is—and this seems to be one of the two or three fundamental issues—that you are not going to succeed with your wiretapping. You can wiretap from here 'til doomsday, but if we don't make effective treaties with Turkey, if the stuff crosses the border from Mexico, if something else happens that I just read the other day, if you continue to have gross corruption, which is inevitable in any drug enforcement effort or gambling enforcement effort, you are not going to wipe out these things.

PROFESSOR BLAKEY: Professor, that really brings up the next question.

PROFESSOR SCHWARTZ: I'm so pleased.

PROFESSOR BLAKEY: And it is the kind of very broad, sort of symbolic question that I was trying to explore with General Clark yesterday. You know ten years ago had approximately 10,000 homicides a year. We now have approximately 20,000 homicides a year. Police efficiency in that area is 85, 90 per cent. Yet there seems to be no demonstrable impact on the homicide rate by police activity. But nobody in his right mind suggests that we decriminalize homicide—

PROFESSOR SCHWARTZ: That is right.

PROFESSOR BLAKEY: —because we have not been successful in eliminating homicide.

PROFESSOR SCHWARTZ: That is right.

PROFESSOR BLAKEY: It may be we are pursuing goals other than the utilitarian goal of eliminating homicide.

PROFESSOR SCHWARTZ: You are absolutely right.

PROFESSOR BLAKEY: What about such things as the narcotics traffic, which some people would describe as the vile exploitation of the weak, the young, the disadvantaged? Maybe the goal being pursued here is a symbolic statement by the society that this is a vile act? Maybe those who prey on other people should be convicted even though we know it will not have an impact on the heroin traffic, and no society could call itself civilized that did not take that attitude.

PROFESSOR SCHWARTZ: I agree with that.

I don't think that is so true of gambling, by the way, the exploitation aspects.

I don't have the impression, talking to people in Harlem and reading about people in Harlem, that they feel very exploited. They feel bitter about the fact that nobody pays very much attention to the gambling that goes on downtown, whereas they are playing numbers—

PROFESSOR BLAKEY: Gambling is different from narcotics.

PROFESSOR SCHWARTZ: Yes, I think that's right.

PROFESSOR BLAKEY: So I am raising—

PROFESSOR SCHWARTZ: But again I think one of the most pernicious concepts is the notion—I'm sorry she isn't here because I wanted to say it to her myself—the notion of fighting fire with fire which Judge Shientag used yesterday in conversation with Mr. Clark.

I don't think we have to use wiretap in order to get into drug traffic and to maintain that symbolic—and perhaps more than symbolic—aspect. Because I do believe, as I am sure you do, that where we are dealing with people who do exploit others' misery, there is a community interest in saying to these people, "We can't catch you all; we can't stamp it out. But if we find out we are not going to let you get away with it."

PROFESSOR BLAKEY: You agree with me, then, the failure to stamp out the traffic is no indication that the law enforcement effort is "a failure?" It may be a success—forget the wiretapping question for the minute—just the law enforcement program.

I am trying to get you to the question of the measure of success.

PROFESSOR SCHWARTZ: It seems to me that is precisely the problem. We have not had any success in dealing with the narcotics problem. It is, as Mr. Clark said yesterday, quoting from the *New York Times*, worse than ever. It got better for reasons having nothing whatever to do with law enforcement, what happened in '69 and '70 and in Turkey and other things, which I think did have to do with law enforcement abroad.

But my point is that what we are talking about is, if you will, the symbolism of a society, and what price symbolism if part of that symbolism is Collinsville, Illinois and Winthrop, Massachusetts, and various other things like that.

PROFESSOR BLAKEY: There is an old symbol, isn't there, the symbol of the top hood who gets away?

PROFESSOR SCHWARTZ: I'm sorry.

PROFESSOR BLAKEY: The top hood who gets away and profits on the misery of other people and whom society never sanctions?

PROFESSOR SCHWARTZ: Sure, and that is going on all the time. And what I am saying is that in effect you are fighting fire with fire or, to use Clark's version yesterday, which I preferred, equally alliterative, you are fighting one form of perhaps private Fascism with another form of Fascism, public Fascism—again misusing "Fascism" to some extent.

What you are doing is saying, "We will use dirty business to go after dirty business."

And I don't think we should do that, because I think that there is a big difference between the mugging that takes place and the exploitation that takes place by a private person and, if you will, the mugging and exploitation that takes place by the community.

That doesn't mean we shouldn't try to do as much as we can about that first forum. But it means that we pay a heavy price, a very heavy price when we go on to the second.

PROFESSOR BLAKEY: Let me shift the discussion somewhat.

PROFESSOR SCHWARTZ: How long are we going to go on?

PROFESSOR BLAKEY: The annual report has cost data on wiretaps. To make a careful analysis of that cost data, don't you think we ought to have cost figures for typical investigations?

In other words, how can we judge whether a wiretap for \$15,000 is expensive unless we know how much typical investigations without wiretaps cost?

PROFESSOR SCHWARTZ: Yes.

PROFESSOR BLAKEY: Would you agree with me?

PROFESSOR SCHWARTZ: I think that is a very good point, and it is something I want to think about some more. It was mentioned to me yesterday in private conversation with Mr. Lipman, and I think that is a very interesting question.

PROFESSOR BLAKEY: For example, some of the staff investigations indicate that there has been limited time and motion study done of at least one strike force, in Chicago, and—I am quoting from memory—it indicates that the rough cost of all investigations, successful and unsuccessful, on the Federal level in the strike force, is approximately \$200,000 each.

What I am concerned about here is the context problem. If I look at \$15,000 and match it against my income and my needs, that is an enormous amount of money. But if I match it over against a program that is spending approximately \$200,000 per investigation, in fact that \$15,000 figure is not terribly large.

PROFESSOR SCHWARTZ: I think, as I think about it now, as you talk, that is a misleading kind of match. Because I think a good case can be made for the proposition that perhaps that \$200,000 is an outrageous figure.

Because the real question, it seems to me, is not \$15,000 as against \$200,000, but what have you gotten for your \$200,000? What have you gotten for your \$15,000?

And if I look at a report by Mr. Nadjari—take an expensive example—in which he says, “I spent X hundred thousand dollars”—and I figured out he spent \$600,000 or \$700,000 in one year, and winds up with seven convictions, three misdemeanors, ending up in fines or 30 days or something, that doesn't strike me as a valuable use of social resources if I think to myself about that \$600,000 or \$700,000 or \$800,000, maybe I might have spent that money on, to take a hearts and flowers example, hot lunches for kids.

Because there is no doubt there is a much weakened Federal lunch program at the same time as we have a much bigger Federal law enforcement program.

And so I am not sure that that is the appropriate measure, the \$15,000 versus the \$200,000.

PROFESSOR BLAKEY: No, I would argue that within the law enforcement context we ought to measure the \$15,000 against the \$200,000, but having gotten that, we should look at what is the cost of a new airplane carrier, what is the cost of a new school, and the cost of X strike force investigations, and set our social priorities on that basis.

PROFESSOR SCHWARTZ: Yes.

PROFESSOR BLAKEY: But just talking about \$15,000 as a lot of money unless we put it in context is not terribly meaningful, is it?

PROFESSOR SCHWARTZ: Pathetic as my analysis is in the cost area—

PROFESSOR BLAKEY: That is all you had to work with.

PROFESSOR SCHWARTZ: That, plus a little imagination.

PROFESSOR BLAKEY: And my commentary may well be on the reporting provisions. It produces misleading data.

PROFESSOR SCHWARTZ: I don't think they include what to me seems quite significant, which is the lawyer's time and everything else in handling the stuff.

Let me add one other thing. If I see, as I indicated in my prepared statement, that this item produced six convictions of \$650,000 on the average, at least, and in each of those six convictions a \$100 fine was imposed, it is going to take a real exercise of imagination and persuasion to persuade me, and I guess others as well, that that was a valuable use of that \$750,000 or who the tap was.

PROFESSOR BLAKEY: It would depend on who the defendant was.

PROFESSOR SCHWARTZ: If that defendant got away with a \$500 fine, I don't care who he is.

PROFESSOR BLAKEY: Suppose he is the Vice President of the United States who, as a result of a case, pled guilty to a misdemeanor?

PROFESSOR SCHWARTZ: Oh, I will grant that as an exception, but I am talking about the average gambling thing.

PROFESSOR BLAKEY: Gambling is one but what about bribery? I would have spent a lot of money to undo one corrupt judge, but very little money to undo one gambler.

PROFESSOR SCHWARTZ: I would, too, but that is not what you have. You have gambling cases.

PROFESSOR BLAKEY: There are two conclusions we could draw from that. One, we could eliminate the statute. The second would be to knock off gambling and start working narcotics.

PROFESSOR SCHWARTZ: The narcotics are much, much more expensive, and then I'd have to figure out what we get when we get narcotics people. Are we getting street people, addicts, pushers? We need a qualitative analysis. So far we haven't had that, and I am curious about the fact that there are, over the six years of the act since the Federal aspect went into operation—I am curious about the fact that there have been, according to my calculations, only 149 drug installations over the six years.

MR. LIPMAN: Federal.

PROFESSOR SCHWARTZ: And in '74 it was the lowest it's been since 1969, except for 1971 when it was 21, and this past year it was 22.

PROFESSOR BLAKEY: Our record contains a number of very sophisticated answers to that.

PROFESSOR SCHWARTZ: And the other thing that goes along with that in terms of consistency is the state figure which started out very high on narcotics and has shifted to gambling.

PROFESSOR BLAKEY: Let me move on to another question, really Professor Remington's question that you responded to a bit this morning. I guess I should preface this by saying you are not really the person to ask it of. I know of your own work in "stop and frisk," and your work in the area of wiretapping, and your position in the American Civil Liberties Union, but let me ask you anyway to comment on what you see as the broad trends in our society as opposed to your personal position and the position of the union.

Don't you see a bit of class bias in opposition to wiretapping that doesn't appear in opposition to "stop and frisk?"

Look at the furor that can be raised in Congress and among prominent people, newspaper reporters, as to wiretapping. And the similar concern is not posed when "stop and frisk" comes along.

PROFESSOR SCHWARTZ: I'm sorry, but I don't think that is true.

In the first place, if we are going to talk about the national legislative forum, the "stop and frisk" issue never came there. The analogous thing that came to it was "no knock," and I would suggest there was a very great furor over that, and it has since been repealed, as you know.

So I don't see that.

I especially don't see that, if I may interject a personal note, in my own position here. I don't know if I am consistent or what have you, but I have never had an indication in the academic world that the people who shared my views on wiretapping didn't also share my views on "stop and frisk," and on other social issues such as integration and the like.

As you may know my personal experience, I have worked in the South. I have worked in school segregation matters in the North. And I don't think there is any sort of mutual exclusivity among them which implies a class bias.

And I do think, in all honesty, that part of the response I tried to set out this morning in my initial remarks, to the effect that opposition to wiretapping is based on political concerns—I do think that cuts across all classes. Because I think one of the central issues of our time in this country is the issue of race and class. Particularly if times remain hard, one of the great questions that this society will be faced with and which, I am unhappy to say, is facing in the wrong way, is what we do about those of our people who don't have jobs and don't

have enough to eat and don't have meaningful lives because of that?

And as this continues there will be more and more dissension. I don't know if we will reach the furor and turmoil of the late '60's and early '70's but there is simply no doubt that the whole wiretap-informer apparatus in the FBI was aimed as much at black people, poor people, poor people's groups, as it was at others.

And the quintessential example of this, of course, is the Martin Luther King tap.

PROFESSOR BLAKEY: Let me say while I can't associate with all of what you said, certainly the deep feeling you have expressed as to the issues facing society with race and class and how they will be exaggerated in the coming years is something that I also very deeply share.

PROFESSOR SCHWARTZ: I'm sure.

PROFESSOR BLAKEY: And I would hope that this record makes it very clear that our disagreements in the past on wiretapping are no indication that men of good faith cannot disagree on wiretapping and also agree on those other issues.

PROFESSOR SCHWARTZ: Yes.

PROFESSOR BLAKEY: Indeed, I might add a personal note. My own feeling about wiretapping grows, in many ways, out of a deep sense of compassion for those people who are exploited in the ghetto by organized crime. And it is my desire and my hope that these people no longer be exploited, and I will, if I can, arm law enforcement with the tools they need, or at least I think they need, to do the job. And I would hope those tools would never be turned to suppress those same people.

Let me move on to a less personal and less deep question.

You have on a number of occasions in the literature spoken about judge shopping.

PROFESSOR SCHWARTZ: What is that?

PROFESSOR BLAKEY: Judge shopping.

PROFESSOR SCHWARTZ: Yes.

PROFESSOR BLAKEY: Professor, you know like I know the criminal system is a series of subsystems, where people who can get warrants from an easy judge still have to face a motion to suppress, and while they may be able to choose their judge for the warrant, the normal judicial rotation system dictates they cannot choose their judge at trial for a motion to suppress.

As a practical matter, then, does judge shopping make any real difference?

PROFESSOR SCHWARTZ: Yes. It make an enormous difference, and I have seen this in conversations with judges.

Judge A issues a warrant. His judge of a coordinate jurisdiction is not going to go around and say

that Judge A was wrong and did a rotten job, especially in light of *Ventrasca*, but it's certainly true.

I remember one judge said to me, a local judge in Buffalo, a state judge, "You know, Herman, I have this terrible problem. I have Judge X's warrant in front of me"—a guy he eats lunch with every day—"and I don't know what to do." He said it was clearly a rotten warrant. The judge who issued the warrant is the one I said in my report had been judge shopped and issued 18 and 20 warrants all of which were thrown out in various forums, including one in Pennsylvania.

He said, "It is a terrible warrant, but I can't say that he did wrong."

"On the other hand," he said, "I think I can find something in the manner of execution which will make it possible for me to knock the thing out."

This happens to be a particularly liberal judge. Not that many judges are going to do that. Most judges are going to say, "If my lunch partner, Judge X, issued it, it's good enough for me."

PROFESSOR BLAKEY: Is this true when those cases are appealed?

PROFESSOR SCHWARTZ: I can't answer that. I don't know. My guess is that the odds are that it often is. As you know and I know, if some evidence is turned up, judges are very loathe to apply the exclusionary rule. And the more that is turned up, the more unwilling they are.

PROFESSOR BLAKEY: Doesn't the prosecutor or policeman who is conviction-minded run a substantial risk if he judge shops, the risk, in short, that he will get that liberal judge at trial? What I understand to be the typical attitude of the appellate courts, moreover, is that there is no reluctance to reverse on a search-and-seizure question.

Isn't he better off, not because he believes in the Constitution, but because he believes in the safety of his conviction, not to judge shop?

PROFESSOR SCHWARTZ: I somehow see that as a world that I am not familiar with. The world I am familiar with is one in which lawyers have traditionally gone to judges whom they trust and whom they can expect to get easy treatment from.

I once asked Judge Mathew Levy, now dead, when New York had its wiretap statute—I said to him way back in the early years, "Judge, tell me how many wiretap applications do you get a year?"

He said, "Oh, one every year or two years."

I said, "How come?"

He said, "When they come in to me, I bring in the sergeant and the captain and give them the whole business, and they don't come to me very often."

I know the judges who issue the warrants. It is to some extent in the administrative reports, with, of

course, the correction about why they go to Judge Klingfeld in New Jersey.

But it just is contrary to my own experience. Any lawyer worth his salt judge shops. I do it in trying to get favorable judges for my civil rights cases. And prosecutors do it. And I don't worry about what is going to happen on appeal if I get a bad panel.

And by the same token, I think I really disagree with you. I don't think that Federal appellate judges, and especially not state appellate judges, are quick to throw out warrants if they have got some defendant who has been convicted. It is just not my own experience.

I don't know that my experience is as extensive as yours, but this is the kind of thing that would show up in reading appellate cases, of which I have read a great many.

And I'm sorry; I don't share that experience.

PROFESSOR BLAKEY: I suppose there is one clarification on the annual reports that ought to be noted at this point; to wit, except for a few judges, none have indeed denied orders. But our record indicates that the place where they are being denied is at the prosecutorial level.

PROFESSOR SCHWARTZ: Yes.

PROFESSOR BLAKEY: Unfortunately, the annual statistics didn't include prosecutor denials. If they had, it would look like a substantially different picture.

Would you agree with me that the report to that degree is misleading?

PROFESSOR SCHWARTZ: I am not sure I know what prosecutor denials are. I know what it means in language, but I don't know what it means in operation.

Essentially, I take it that means that the police have some evidence and go to the prosecutor and say, "Will you get us a warrant," and the prosecutor says, "You don't have the fellows; I am not going to do this."

In other words, the prosecutor acts as a screen. That may be, and it may be that that kind of information—not may be—I am sure that kind of information would be helpful.

The whole question of—

PROFESSOR BLAKEY: If the report does not include that kind of information, then it is misleading to draw the conclusion that the judges are simply rubber-stamping from the fact that almost none are disapproved.

PROFESSOR SCHWARTZ: Well—

PROFESSOR BLAKEY: All other things being equal.

PROFESSOR SCHWARTZ: It may be that the judges are rubber-stamping the prosecutors, not that they are rubber-stamping the police.

I may say I have seen some of the Pennsylvania warrants and affidavits. I read a certain number of them in connection with my work on the *Whitaker* case. And they met probable cause standards, but I must say they come pretty close to being boilerplate of each other.

Maybe that is the nature of the enterprise, that one gambling case is much like another. But I looked at the order; I looked at what the judge who, interestingly enough, maybe by his own choice, had issued most of the wiretap orders—the now late Judge Joe Lord, not Joe Lord III, but Joseph Lord, Jr.

And I have read some of his orders. And I didn't get the impression, looking at those, that they had been scrutinized carefully. But on the other hand, these are routine gambling cases. So it may well be, what is there to see once you have somebody who comes in and says, "I know it meets *Spinelli* and *Aguilar*."

The thing I found troublesome was what seemed to me to be clear boilerplate, "The alternate methods have been tried and are too dangerous;" and as I have indicated before, Chief Judge Lord, who is the only judge in America who struck down the wiretap statute, said as he read the legislative history, this was not intended to be too onerous a burden. And it is my impression that is how most judges see it and have not too much of a burden of proving alternate methods of investigation.

PROFESSOR BLAKEY: We'll take a five-minute recess.

[Whereupon, a short recess was taken.]

PROFESSOR BLAKEY: To turn to the question of extensions, you make a recommendation that they should be severely limited. Would you make a recommendation that there be an absolute number on them?

PROFESSOR SCHWARTZ: That is a very complicated matter, and it is one of the problems of what happens when you start playing with pitch; you can't clean your hands of it. I would much rather there were no wiretapping at all. And once you say, "Yes, but we have it," aren't you going to have to allow it for two years or three years, that kind of thing?

In the first place, I think extensions are much too readily available.

PROFESSOR BLAKEY: Suppose I agree with you. How do I limit them?

PROFESSOR SCHWARTZ: In the first place, you rewrite your statute, and you require a fresh showing of probable cause.

PROFESSOR BLAKEY: I think it has one now.

PROFESSOR SCHWARTZ: I don't think so because all it says, "Or a reasonable explanation of why it has not been obtained."

PROFESSOR BLAKEY: But suppose when you put the tap in, the first conversation is, "I am leaving on vacation and will be back in business next Thursday."

PROFESSOR SCHWARTZ: I don't think that is fair because unless you have heard absolutely nothing that week and intruded on nobody's privacy, in which case as a practical matter there hasn't been any wiretapping, then in effect you have a lengthy general search waiting for the person. You don't have a right, I think, under a conventional warrant to go fishing through all the house looking for something if it turns out that you say something is in one room and it doesn't happen to be there.

PROFESSOR BLAKEY: I think it is clear in the statute. If you have one named person, and you didn't have that magic phrase, "and others unknown," and you listened for two days and then he left on vacation, the minimization requirement would say that while you could keep it on that 15 days, you'd have to minimize everybody else out, and since he was gone you wouldn't listen for the next 15 days. Isn't that correct?

PROFESSOR SCHWARTZ: I guess so. But in the first place, you always have "and other persons unknown" because everybody has learned that.

And in the second place, I am thinking of *King v. California* with which you may not be familiar. It was a big marijuana case.

PROFESSOR BLAKEY: A boatload full.

PROFESSOR SCHWARTZ: That is right.

PROFESSOR BLAKEY: Not a rowboat.

PROFESSOR SCHWARTZ: That is right. And the tap was in for 85 days. The judge found that contrary to what the prosecutors had said, a minuscule number—5 per cent, 4 per cent—were, quote, incriminating, close quote.

PROFESSOR BLAKEY: Have you examined that case yourself?

PROFESSOR SCHWARTZ: I have read the opinion.

PROFESSOR BLAKEY: I mean the actual transcript and materials.

PROFESSOR SCHWARTZ: No.

PROFESSOR BLAKEY: That was brought up in prior testimony of a witness before the Commission, and the Department of Justice was asked to comment on it. Their explanation was that the judge probably disagreed with the Department because he wasn't sophisticated enough to recognize coded comments as being incriminating.

PROFESSOR SCHWARTZ: Maybe yes and maybe no. There were five or six extensions, and the reason given was not, "We are getting hot stuff, coded comments," but "The boat hasn't shown up yet, and that is what we are waiting for."

Meanwhile, we are listening to all this other stuff. And it is that kind of thing that troubles me.

As I tried to say in that article back in Michigan, the way the statute is written it is not that different from the New York statute which the Supreme Court condemned, which simply says, "You can have extensions if it is in the public interest," because the public interest is either that we got something and have got to keep going, or we didn't get it but there is a good reason why.

PROFESSOR BLAKEY: Assuming that is the law, which I don't agree it is, would you require a fresh showing of probable cause?

PROFESSOR SCHWARTZ: I checked the legislative history on that and the congressional testimony seems to bear out the notion that that is not required. But I think that was said unthinkingly. In other words, I don't think anybody addressed themselves on the floor to that refinement.

So let me come to your question, an absolute number.

PROFESSOR BLAKEY: Would you support an absolute number?

PROFESSOR SCHWARTZ: Probably, on the theory that the alternative—you win some, you lose some. The alternative is inevitably the kind of stuff you get in New York.

PROFESSOR BLAKEY: Let me give you a law professor's question. You are in on a narcotics tap. You are in the last day of your last extension and you overhear, "Call me tomorrow and I'll give you the name of the informant we are going to hit and where we are going to do it."

PROFESSOR SCHWARTZ: You know, that is a fascinating hypothetical. It comes up in every discussion that I have ever had about anything. Would I allow this if somebody's life were at stake?

Of course, I will allow that if somebody's life is at stake.

Bill Ruckelshaus struck a particularly sensitive chord when he said, "Suppose we got information on the last day of the tap that a synagogue was going to be bombed." And since I occasionally go to synagogue or my father does, that is something I am unhappy about.

Of course, if there is an imminent danger to life and limb, we will allow an awful lot of things. And if that is the way you want to write your statute, that we are going to allow it in any case where there is probable cause to believe an imminent danger to life and limb, sure, I'll go for that. I have no problem with that.

PROFESSOR BLAKEY: Let me give you the next one down the ladder of importance.

Suppose you have been in on a narcotics tap and you have identified most of the major conspirators,

and the last day you hear the guy say, "Don't forget, Mr. Big is calling tomorrow."

PROFESSOR SCHWARTZ: I was expecting those words, "Mr. Big."

Yes, I think that is just one of the prices you are going to have to pay in order to avoid the kind of thing that you get in New York and Queens and Nadjari and everywhere else, because, look, let's go farther, Professor Blakey. I don't want to open up the entire issue again, but I have not said that giving up wiretapping power costs us nothing.

I don't think it costs us very much, but I haven't said it costs us nothing.

But, you know, I know you to be a very devout practicing Catholic, and it seems to me if there is anything that the Catholic Church in its long history has taught us it's that life is a very difficult enterprise, and there always are cruel choices that have to be made, sometimes between good and good and sometimes between bad and bad. There is a price to be paid.

And I think in order to avoid what seems to me to be a greater evil, in order to avoid the highly improbable likelihood that we will lose very many Mr. Bigs by something happening on the last day of the tap, I would much rather avoid the very high likelihood, which we already have from experience, of taps that are in for 200 days, 100 days, 90 days, 60 days, 30 days, when it seems to me absolutely clear that the Supreme Court in the *Berger* case meant not to allow that kind of thing—apart from policy.

PROFESSOR BLAKEY: Let me raise a related area.

The recommendation has been made to us that the absolute limit of the initial surveillance, which after all is an upper limit, be limited to, say, 15 days.

PROFESSOR SCHWARTZ: Yes.

PROFESSOR BLAKEY: The issue has also been raised with us of making the progress reports mandatory.

PROFESSOR SCHWARTZ: Yes.

PROFESSOR BLAKEY: Would you support lowering the absolute limit from say, 30 to 15?

PROFESSOR SCHWARTZ: Well, actually, I heard some of that exchange this morning. And as I sat there listening, I thought to myself that I think my approach would be rather different, and probably somewhat less to your liking.

I thought the questions that the Chairman asked about what goes on during that supervision were very good questions. Does he cut them off if he doesn't find anything? Some judge thought it was worth 15 days and assumed that maybe nothing would happen the first five days; otherwise, why give them 15?

What I have suggested, I think in the Roscoe Pound piece, was five days.

PROFESSOR BLAKEY: Would you want progress reports in five days?

PROFESSOR SCHWARTZ: No, you get a progress report in effect when you go back for an extension. And I'd give a few extensions and put an upper limit of, say, five or four. So that means I'd wind up in total, for any given wiretap, with 20 days, 15 days.

PROFESSOR BLAKEY: And no progress reports.

PROFESSOR SCHWARTZ: Well, you have the progress report—no progress report as we currently understand the progress report—instead an extension application which would meet the fresh probable cause and that business.

I was impressed by the fact that the New Jersey people seemed to have made many important gambling cases in a few days—I am not sure of the criteria of importance.

Certainly in the gambling area, I just realized, there is a difference. There is a difference between Federal interception and state interception, because the Federals are really looking for the jurisdictional handle, and that may not come the first, second, third, or fourth days. Obviously, the state prosecutor doesn't need that handle.

All of which goes to say we don't need Federal wiretapping again.

PROFESSOR BLAKEY: The issue that I am raising with you obviously is the interrelationship between progress reports and the length of time.

Let me kind of pursue with you—assuming we say with a relatively longer period of surveillance—

PROFESSOR SCHWARTZ: Yes.

PROFESSOR BLAKEY: What sorts of recommendations should the Commission make about those progress reports? Should we say they should be every five days? Should they be the third day? The ninth day? The 15th day?

In other words, once the surveillance is in and you get back a favorable progress report, indicating the objectives are being attained, is the need for continued supervision as pressing as it is in the early stages?

PROFESSOR SCHWARTZ: You know, I find that real hard to answer, because I don't know enough about the progress reports, their significance. I would have been, and am, frankly, kind of surprised if they amount to very much as a check.

Currently, on the state level it is nonexistent. What does the Federal judge do with progress reports every five days? I do know that very often they are oral; they are telephone calls, saying, "Yes, we are hearing a lot."

PROFESSOR BLAKEY: How comprehensive should we require them to be?

PROFESSOR SCHWARTZ: I think you've hit on an area that I haven't really thought very much about, and I am not at all sure that any thoughts I might have would be particularly useful to you.

PROFESSOR BLAKEY: Particularly at 4:00 o'clock.

PROFESSOR SCHWARTZ: Particularly at 4:00 o'clock.

PROFESSOR BLAKEY: Let me turn to the last area which, fortunately, for all of us and particularly the reporter, is shorter.

A number of people who have testified before the Commission have recommended changes in the inventory procedures.

PROFESSOR SCHWARTZ: Yes.

PROFESSOR BLAKEY: As the statute now reads it says, "To the subject and to other such people as in the interest of justice."

PROFESSOR SCHWARTZ: Yes.

PROFESSOR BLAKEY: And the recommendation has been made that we require notice to be routinely given to all people, to all identifiable people, and to all identified people. Other suggestions have been made that perhaps we should, in cases where surveillance is declared illegal, make the police give notice to everyone, too; but in cases where there is no indication that surveillance is illegal, that the number of inventories filed should be relatively restricted.

At least three rationales have been offered for restricting the notice requirement. Once one is overheard, and you learn your conversation was overheard, as you talked to another, there would always be a potential rupture of your relationship with that person. You'd learn he was being investigated for a crime. That is one counterproductive result of the notice requirement.

Second, that the very process of the government noticing a person may be an invasion of that person's privacy. The illustration given once before was a notice that in a prostitution case was given to all the "Johns." In some cases, the wives came into possession of the notices, and to put it mildly, this caused some consternation.

I suppose I can see the same sort of a result in a gambling case where a wife, not being aware of her husband's betting habits, might be disturbed.

The last is the problem of computers and names, that once a person not normally identified in a tap was identified, he would then go into the central index. He would have to be there for the purpose of notification, and he would have to be there to respond to that famous question, "Have I ever been overheard?"

This would mean a large number of people who might not normally be in that index would be put in that index, and maybe it is not a good idea to collect a large number of names in the files.

That is a very broad description of where we are in our analysis of the notice question. I wonder if you'd share with us your thoughts on that.

PROFESSOR SCHWARTZ: I think those considerations, though I think they all are worthwhile, are not of the greatest importance. To be perfectly honest, I can't get overly excited about the man's wife learning about it. I must say I receive an enormous amount of mail my wife hasn't the vaguest knowledge of, and I don't see why this should be any different. And I think that is a rather mild consideration to set off against the problem that very often the person who is overheard and identified may be the one who has the most interest in challenging what may be an illegal tap.

I also don't think that it should be restricted to illegal taps, because very often taps which don't pan out may have been illegal in inception but nobody ever knows. That is part of the problem.

PROFESSOR BLAKEY: It is not nobody. At least the subject knows.

PROFESSOR SCHWARTZ: If the subject knows and the subject is involved in things he would rather not fuss about, he may not fuss about it, just let it go.

I think that the question of the going into an index—you honestly touch a sensitive spot for someone like me.

I don't know how to get around it except that that may be part of the price that is paid, a price that may become very important for that very person if subsequent actions are brought against him, in which case he may want to know.

Because certainly, as I think you may have seen in the Times a couple of weeks ago, John Crewdson's piece on the taps in the Ellsberg case, which are very serious problems and have created serious problems, particularly in the area of political surveillance.

And I have a feeling that we will willy-nilly have that kind of stuff with us in one form or another, whether under Title III or otherwise—and if it is not otherwise, then I think emphatically under Title III, you can rest assured of that.

Then the consideration of rupture of relationships—I have a feeling that it is possible to notify people, "You have been overheard on a wiretap"—I'm not sure—I was going to say without necessarily divulging a great deal of information about that tap. And if you are interested, you will go ahead and ask for more. Most people won't be interested. So in other words it may be that a notice

which simply says, "In connection with law enforcement of someone and persons unknown, you have been overheard. Should you wish more information or to challenge the legality of that overhearing, we would be pleased to furnish you with the relevant information."

My guess is that 99 people out of 100 would say, "Oh, my God, I don't want to have any more to do with it."

PROFESSOR BLAKEY: Do you think—

PROFESSOR SCHWARTZ: Let me just add one more thing. On this issue of the rupture of relationships, I don't really know. I have known a great many people—

PROFESSOR BLAKEY: Some of whom would be proud to be overheard?

PROFESSOR SCHWARTZ: Well, as a matter of fact, some of them were quite dismayed that we didn't come up with some of these things.

No, I think that is true. I have known a great many people whom I have assumed were overheard, and it hasn't affected my relationship with them in any way.

PROFESSOR BLAKEY: Professor, you have been a man not only of courage, but endurance.

PROFESSOR SCHWARTZ: Thank you.

PROFESSOR BLAKEY: I appreciate your candor. What you have set out in the record today will be useful not only to the Commission but to all our future students to whom you will assign this material. Thank you.

The meeting is adjourned.

[Whereupon, at 4:07 p.m., the hearing was adjourned.]

STATEMENT OF
PROFESSOR HERMAN SCHWARTZ,
STATE UNIVERSITY OF NEW YORK, BUFFALO

Thank you for inviting me to participate in your deliberations, both in my personal capacity and on behalf of the American Civil Liberties Union. Our views on this matter are not, I am sure, unknown to you, and they have been expressed in many articles and papers. I am therefore taking the liberty of submitting to you my most recent comprehensive paper on the subject, that given at the American Trail Lawyers Foundation conference last June in Cambridge, Massachusetts, together with a copy of my 1973 report for the American Civil Liberties Union; the latter contains most of the statistical and other analyses underlying that paper.

In this testimony, I shall try to do four things: (1) update some of the statistical data in my two submissions; (2) examine in some depth the electronic surveillance operations of New York State Special Prosecutor Maurice Nadjari; (3) comment on some current efforts to place some limits on certain kinds of surveillance; and (4) make a few recommendations about the current reporting operations under §2519 of the statute by prosecutors, judges, and the Administrative Office of the United States Courts. For lack of time, I have been unable to develop the

detailed analysis of the state data beyond 1972 in all cases, but I have updated the federal data as much as I could.

Let me first summarize my position as baldly as possible: I think electronic surveillance has not been shown to be of any significant value in reducing crime rates or otherwise coping with our troubling criminal problems; it costs a great deal in both liberty and money; these facts were known to the proponents of the legislation; whether intended or not, the legislation served primarily to direct attention from the very real social problems that underlie crime in a community and to lull people into thinking that tinkering with our criminal justice

system and giving up some of our liberty could have a beneficial impact on the quality of life in our country.

I. The Data Updated

There are two basic questions in any analysis of the question: (1) How much does electronic surveillance cost us in (a) a loss of privacy and (b) an expenditure of money? (2) What have we gotten for that expenditure? The following charts set out the amount of privacy invasion.

TABLE 1
FEDERAL AND STATE SURVEILLANCE

Year	Orders Authorized	Installations	People	Conversations
1968 (6 mos.).....	174	167	4,250	62,291
1969.....	302	290	14,656	186,229
1970.....	597	590	25,812	373,763
1971.....	816	792	32,509	496,629
1972.....	855	839	42,182	517,205
1973.....	866	812	^a 39,788	^a 495,320
1974.....	728	694	^a 40,946	^a 589,900
Total	4,338	4,184	200,143	2,721,337

^a Approximate figures based on multiplying averages in 1974, Table 4.

TABLE 2
FEDERAL SURVEILLANCE

Year	Orders Authorized	Installations	People	Conversations
1969.....	33	30	4,256	41,929
1970.....	183	180	10,158	143,508
1971.....	285	281	15,099	256,720
1972.....	206	205	13,352	209,715
1973.....	130	130	9,460	113,360
1974.....	121	120	5,760	111,480
Total	958	946	58,085	876,712

TABLE 3
STATE SURVEILLANCE

Year	Orders Authorized	Installations	People	Conversations
1969.....	269	260	10,400	144,300
1970.....	414	410	15,654	230,255
1971.....	531	511	17,410	239,909
1972.....	649	634	28,830	307,490
1973.....	736	682	30,328	381,960
1974.....	607	574	35,186	478,420
Total	3,206	3,071	137,808	1,782,334

TABLE 4
FEDERAL AND STATE INSTALLATIONS BY CRIME

Year	Gambling	Drugs	Homicide ^a	Kidnapping	Other
Federal					
1969.....	20	4	0	1	5
1970.....	120	39	0	0	21
1971.....	248	21	0	0	12
1972.....	147	35	0	0	23
1973.....	81	28	0	0	21
1974.....	67	22	0	2	29
Total	683	149	0	3	111
State					
1968.....	18	68	20	1	60
1969.....	78	80	19	1	82
1970.....	204	84	20	0	^b 95 + 7
1971.....	304	104	18	1	84
1972.....	340	193	33	0	^b 68 + 7
Total	944	529	110	3	^b 389 + 7

^a Includes attempts, threats, solicitations and conspiracy to commit homicide (including manslaughter) as well as a few instances of consummated murder.
^b Not indicated.

TABLE 5
COSTS

Year	Federal	State	Total
1968.....		\$200,000	\$200,000
1969.....	\$440,287	470,000	910,287
1970.....	2,116,266	938,000	3,054,226
1971.....	2,114,216	1,502,340	3,616,556
1972.....	2,007,975	2,562,860	4,570,835
1973.....	1,603,680	2,890,656	4,494,336
1974.....	1,302,840	4,309,538	5,612,378
Total	\$9,585,264	^a \$12,873,394	\$22,458,618

^a This figure may be high by \$40, but time pressures have precluded finding the error.

TABLE 6
FEDERAL CONVICTIONS BY OFFENSE

Year	Gambling	Drugs	Homicide	Kidnapping	Other	Totals
1969.....	108	55	0	0	4	167
1970.....	274	126	0	0	14	414
1971.....	519	45	0	0	40	604
1972.....	496	109	0	0	21	626
1973.....	65	54	0	0	43	162
1974.....	3	42	0	1	5	51
Total	1,465	431	0	1	127	2,024

TABLE 7
STATE CONVICTIONS: OVER-ALL ^a

Year	Total	Federal	State
1969.....	408	267	241
1970.....	1,097	414	683
1971.....	1,723	604	1,119
1972.....	1,926	626	1,300
1973.....	1,016	162	854
1974.....	179	51	128
Total.....	6,349	2,024	4,325

^a The difference between total annual convictions and Federal convictions from Table 13, 1974 Report.

It will be noted that as the federal amount declines, it is gambling which is declining the most; the figure for 1974 drug installations is about what it was in 1971, the highest federal wiretap year, but gambling has fallen from 248 to 67, almost 75%; the "Other" category has more than doubled, but the absolute number is still low.

Interestingly enough, the average combined federal-state cost jumped from \$5,632 in 1973, when the federal average was \$12,238, to \$8,087 in 1974, when the federal average fell to \$10,857, making it clear that the state costs rose substantially. Why federal costs did not rise in view of inflation is not clear.

Some of these interceptions are very expensive. Thus, some 32 federal installations in 1973 exceeded \$15,000 and many by a great deal. I was startled to note that of these, some 18 have not yet been associated with a conviction, or an arrest, though it may be too early for many convictions—the 1975 figures will tell that story. It is not too early for arrests, however—these generally come in the first year and certainly by the second. See Administrative Office Table 13 of 1974 Report, p. XXII.

Costs per conviction are reliable only for years up to 1972, since it takes approximately 22 months or more to conclude most cases. To get an idea of cost/conviction, I have therefore calculated the costs up to 1972 and divided that by the number of convictions through the 1972 surveillance:

TABLE 8
COST PER PERSON CONVICTED

1969-72 Federal cost:	\$6,678,744
1969-72 convictions:	1,811
Cost per conviction:	\$3,688

This figure jibes with some of the annual computations I have made, which run at about \$3,250 for 1972 convictions, \$3,500 for 1971 convictions. It should be noted that the drug surveillance is generally much more expensive than the other kinds.

It may also be worth noting that the large majority of installations—many of which are quite costly—have apparently produced nothing. The federal figures for 1971 and 1972, for ex-

ample, where we have relatively complete figures, show that almost two-thirds of the installations produce nothing:

TABLE 9
INSTALLATIONS ASSOCIATED WITH FEDERAL CONVICTIONS

Year	Gambling	Drugs	Other	Total
1971.....	86/248	6/21	8/12	100/281
1972.....	51/147	15/35	5/23	71/205
Total.....	137/395	21/56	13/35	171/486

II. The Special Case of Maurice Nadjari

Few prosecutors have ever taken on an assignment with so much public support as Maurice Nadjari, the New York Special Prosecutor against Corruption; he was even given his own judge, New York State Supreme Court Justice John Murtagh, to try the cases developed by Mr. Nadjari. And right from the beginning, he made clear—like a well-trained alumnus of former New York District Attorney Frank S. Hogan's office—that he would rely heavily on electronic surveillance. And he has: in 1973-74, he installed 56 surveillances, kept them in for substantial periods of time and at great expense.

It is still too early to make a full assessment of the results of this activity, but so far, little seems to have been accomplished. If this tentative and preliminary conclusion is borne out by the 1975 and 1976 reports, then it will be clear that electronic surveillance is not a terribly useful tool for perhaps the most important area where it is said to be needed—official corruption.

And the early returns are not very favorable. Although I have elsewhere stated that I don't think arrests are a very good indication of success, the absence of arrests in the first two reports for a surveillance usually means there won't be many more.

Mr. Nadjari's 1973 *taps* apparently overheard 1,416 people, of which, according to Nadjari's own report, only 30% were incriminating. A very high proportion of these people and conversations may well have been involved in lawyer-client or judicial-business conversations, since his prime target is corrupt judges.

These surveillances were extremely expensive: the 24 surveillances reported in 1973, one of which didn't work, cost about \$282,000, which approximates the federal amount. One tap cost \$109,946, was in operation for 85 days, overheard 123 people in 625 conversations, and has yet to produce a single arrest; as indicated earlier, if a surveillance isn't associated with an arrest within the first two years, it usually won't be.

It should also be noted that many of Mr. Nadjari's taps were in for quite long periods of time—an average of 40 days, with a high proportion in for 90 days, and some for much longer.

So far, the 1973 taps have produced only 7 convictions—2 for obstructing governmental administration, a misdemeanor; 1 for possession of a dangerous weapon, which is usually a misdemeanor; 2 for what may be gambling; 2 for bribery. There have been only 15 other arrests—plus 12 by other law enforcement agencies for which Mr. Nadjari's responsibility is not stated—and perhaps these will produce additional convictions.

In 1974, the average cost per order was almost \$20,000, making his electronic surveillance bill equal to \$620,000, a very high figure, indeed. So far, this has resulted in 25 arrests, again a meager number but perhaps it is too early. The reported taps have been in for very long periods indeed. The first twelve reported apply to 1973, and these include surveillances of 320 days, 127, 240, 270, 210, and the like; they were associated with some 16 arrests. The 19 installed in 1974 were for much shorter periods. The average for the 1974 reports was 70 days.

It will be important to watch the Nadjari operation closely, for he has used electronic surveillance very extensively in an area the importance of which is indisputable, unlike the other areas where wiretapping is extensively employed. Many questions have already been raised about the effectiveness of his performance to date. See Tracy, "From Super Cop to Super Flop," *The Village Voice*, 3/17/75, p. 5. His performance will, of course, be measured against that of Judge Herbert Stern of New Jersey, who was extremely successful against corruption without reliance on electronic surveillance.

III. Consent Surveillance by Lawyers

The statute is very ambiguous about consent surveillance by private people. Section 2511(d) makes criminal liability turn on whether the consent interception is with "tortious" intent, or for the purpose of "committing any other injurious act." This would seem to make criminal liability turn on the vagaries of tort law in the first instance and to go even further—to make it turn on some totally nonspecific meaning of "injurious." This section of the statute could well be void for vagueness under standard notice principles recently reaffirmed in a series of cases, of which *Papachristou v. City of Jacksonville*, 405 U.S. 156 (1972), is probably the most prominent.

My own feeling, expressed many times, is that consent surveillance is probably a useful tool of law enforcement, can be limited to very specific targets, and time periods, and does not strike at speech and association the way third-party surveillance does. It is really part of the more general problem of the use of informers and betrayal for law-enforcement purposes, a tactic which may well be a necessary evil in some circumstances but is unquestionably an evil.

Recently, there have been certain Bar Association opinions on the ethical propriety of a secret recording by a lawyer, or under a lawyer's supervision or instigation, of a conversation with another person, be it another lawyer, a client, a witness, or an adversary. The Arizona option, and perhaps the Colorado one as well, seems to prohibit a prosecuting attorney from such recording, either directly or indirectly, without notifying the adverse party or lawyer.

What is novel about this opinion is that it holds prosecutors to the same ethical standard as other lawyers are held to, a sharp departure from traditional practice. Regardless of *Berger v. United States*, 295 U.S. 78, 88 (1935), and similar pronouncements in the Code of Professional Responsibility, EC 7-13 and elsewhere, prosecutors are generally allowed to engage in unconstitutional and unethical practices, when similar action by private lawyers would bring swift retribution; the most the prosecution faces is an occasional reversal, often in a weak case. See Alschuler, *Courtroom Misconduct by Prosecutors and Trial Judges*, 50 Texas L. Rev. 630-76 (1972). I do think that if there is a very real necessity for such a surreptitious recording, it should be done pursuant to a court order and under strict limitations.

IV. Suggestions about Reporting

The Administrative Office Reports are very helpful, but could be more so. For example:

(1) They should break out the federal and state subtotals for such matters as convictions, etc.

(2) They should indicate what the convictions were for, where the conviction occurs in the same year as the interception.

(3) They should provide more information about specific crimes and surveillances related to them.

In short, they should try to refine more of the information already in the reports, which I have tried to develop crudely and imperfectly on my own.

The staff has also asked me to comment on an exchange of letters between General Hodson and the Administrative Office of the United States Courts on a range of very important issues.

Costs: In my analyses, I too have been troubled by the almost whimsical manner in which costs seem to be reported. The variations that I have found from state to state, between state and federal figures, and among federal figures, see my 1973 ACLU report, seem much too great. In addition, I do think that the total cost and value of the wiretap experiment simply cannot be evaluated without some estimate of how much in lawyers' and judges' time is spent preparing and litigating the papers. Contrary to the Administrative Office, I think it is a significant figure, and I think a general estimate could be arrived at. It doesn't have to come down to specific dollars and cents, an estimate would be enough.

Accuracy and Comprehensiveness: I do not fully understand the Administrative Office response about the link between cost and sentence. One cannot usually evaluate the value of a surveillance until several years after installation anyway, so what's the problem about the different reporting years for costs and sentences? And though one can't fully determine the significance of a sentence without knowing the statutory maximums and minimums, one can still conclude that a 90-day sentence or probation implies that the offense is something less than horrendous, regardless of the maximum.

Consensual Eavesdropping: I don't understand why the Office can categorically say, "The volume of this type of wiretap would prohibit reporting"—it hasn't been tried, so we really can't know.

Finally, computerization really seems to be the only intelligent way to handle this problem, if the coding and programming problems can be taken care of. There is simply too much data and there is too much that one can do with it to forego use of the computer. It can be done with a pencil and paper—I've tried for many years now—but a computer would be far better.

REFLECTIONS ON SIX YEARS OF LEGITIMATED ELECTRONIC SURVEILLANCE

by Herman Schwartz

Professor of Law, State University of New York at Buffalo

Watergate and wiretapping—they even *sound* similar! Rarely have we seen so many ironies, so many boomerangs, so many turnabouts as we have in the last two years, and most of these have resulted from electronic surveillance. The President taps his own brother; Henry Kissinger taps his own staff; the President's secret taping apparatus is used against him; E. Howard Hunt and G. Gordon Liddy reportedly taped their conversations with high White House officials, including the President.¹ The Nixon Supreme Court strikes down the Nixon claim to inherent power to tap dangerous people, in an opinion written by a justice who only the summer before defended the claim; the same Nixon Supreme Court, with four members chosen because of their hostility to letting criminals go free, issues a unanimous ruling on a nonconstitutional technicality that will probably result in the freeing of over 600 alleged criminals because the Department of Justice misrepresented to the courts that John Mitchell had personally seen and approved wiretap applications when he hadn't. And these are only some examples.

It is no surprise that wiretapping and electronic spying have played such a major role in these events. As I will develop later, wiretapping is essentially an instrument of war, used for intelligence purposes primarily. Unlike the more conventional police techniques, it is not really an effective crime detection device, but rather a technique for waging war. And no previous Administration, right from its first days in office, has seen the world, including fellow-Americans, in such war-like terms. "Enemies lists," "national security," "war on crime," "war on narcotics"—the militarist, beleaguered, state-of-siege attitudes reflected in these phrases and concepts are the distinguishing marks of the Nixon Administration.

The Nixon Administration does not, of course, have a monopoly of spying on its enemies. Franklin Delano Roosevelt, one of the most revered names in the liberal pantheon, formally authorized warrantless national security surveillance in 1940;

Robert F. Kennedy may well have been the primary influence in legitimating wiretapping for law-enforcement purposes, though it appears that he ultimately changed his mind; Lyndon B. Johnson apparently listened in on newsmen's calls from the White House, according to a *New York Times* story a while back; governments in France and Italy have also used wiretapping against political and ideological enemies. But as former Nixon speechwriter William Safire put it vividly a few weeks ago, "the willingness to listen in . . . to penetrate personal privacy in order to preserve national secrecy, was second nature to Richard Nixon . . . [He has] an addiction to eavesdropping"²—which apparently goes for John Mitchell, too, as we shall see.

What I should like to do in this paper is (1) track the history of how we came to where we are today, including a discussion of the enactment of the Wiretap Act in 1968; (2) analyze some of the costs and benefits of electronic surveillance for law enforcement purposes, as revealed by the official statistics for six years of wiretapping under the Act, and by facts gleaned from court cases and elsewhere; (3) set forth some thoughts on national security surveillance; (4) offer some reflections on what all this means with respect to the value of electronic surveillance for law enforcement, for national security, and to the national temper and attitude; and finally (5) outline some possible remedies.

I. HOW WE GOT WHERE WE ARE

Several elements recur in the history of the wiretap controversy: (1) electronic surveillance is used primarily for victimless crimes like gambling and prostitution offenses; (2) its usage rises in a period of severe internal discord; (3) people become fearful of crime waves; and (4) the Supreme Court is deeply involved.

All of these were present in the 1920's, the first and still one of the most significant wiretap decades. There had, of course, been a good deal of private and public tapping earlier. The first federal

tap was apparently installed in 1908, when Attorney General Bonaparte allowed his newly-created Bureau of Investigation—which later became the Federal Bureau of Investigation (FBI)—to tap in labor and immigration matters. There was apparently a good deal of private wiretapping in the newspaper wars early in the century, as well as local police surveillance of unions and even priests; the latter occurring in New York which was, then as now, the wiretap capital of the nation.

The 1919-31 and the 1961-72 periods seem the most significant and contain striking parallels. Enforcement of the liquor laws then and the narcotic and gambling and drug laws today have impelled law enforcement officials to use electronic surveillance extensively, for where there are no complainants, the need to infiltrate with either human or electronic spies seems essential. In both instances, as now seems clear, this has been carried out with very little impact. The "Red scares" of the 1920's, and the occurrence of some bombings (the perpetrators of which were never identified) are paralleled to the recent history of attacks on dissenters against the Vietnam War and black militants, and the accompanying violence and bombings. In both periods, there were abuses of the civil rights of political and ideological opponents, including break-ins, raids, abuses of grand juries, and a general indifference to legal limitations by law enforcement. It was during the early '20's that J. Edgar Hoover started his massive card index system of dissenters and dissidents, with Attorney General A. Mitchell Palmer's support. Congressmen and other political opponents were reportedly tapped, in a premonition of Watergate.

In 1924, when Harlan Stone took over the U.S. Justice Department in the wake of the Teapot Dome scandal, he banned all wiretapping, and Hoover went along, calling the practice "unethical." The U.S. Treasury Department also officially opposed surveillance at that time, just as the Internal Revenue Service (IRS) did in the '60's, but in both periods it quietly engaged in widespread surveillance.

In 1927, the Supreme Court gave a constitutional green light to electronic surveillance in the *Olmstead* case.³ The decision is now only a constitutional relic, but in its time—and that time ran 40 years—it exercised a great and pernicious

influence on the development of control of electronic surveillance. Its archaic requirement, that a trespass be committed before the Fourth Amendment was involved, meant that there was no protection against any bugging, and only the feeblest statutory protection against wiretapping.

The thirty years from 1930-1960 saw a great deal of federal, local and private wiretapping and bugging, the application to wiretapping of a prohibitory statute (§605 of the Communications Act) that seems to have been intended primarily for other purposes, and the revival of very extensive surveillance for intelligence and national security purposes. This time the surveillance was on authority from FDR in 1940⁴ but it expanded far beyond his authority by later Presidents and Attorneys General to include, for example, organized crime. After the Supreme Court's construction of §605 of the Communications Act of 1934 to prohibit official as well as private wiretapping, numerous efforts were made in almost every Congress to override that decision, some of which came very close to succeeding. In 1940, Attorney General Robert H. Jackson found a way to get around it by ruling that the prohibition applied only to *both* interception and divulgence and that, so long as the fruits of a wiretap were not disclosed outside the Department, federal agents could continue to intercept.

In information released by Senator Hugh Scott (R-Pa.) last summer in an effort to show that the Nixon Administration has not used wiretapping more than other Administrations, it was revealed that from 1945-47, 1,257 national security wiretaps were installed. It appears also that throughout this period, local police wiretapped extensively both for themselves and for the FBI. There were frequent revelations of electronic surveillance throughout the country during this period, in articles by the National Lawyers' Guild as a result of revelations in the *Judith Coplon* case, by Alan Westin, by the *Reporter* magazine, and in Samuel Dash's monumental study published in the late '50's, *The Eavesdroppers*.

In 1957, there occurred an event which was to transform the situation: the meeting at Apalachin, New York of alleged organized crime figures, which was broken up by New York State Police. Law enforcement authorities now felt they had con-

vincing proof of a massive organized crime conspiracy. J. Edgar Hoover had earlier resisted efforts to bring the Bureau into that area, either because he feared corruption or doubted that he would be able to rack up impressive statistics. After Apalachin, however, he began to tap and bug to make up for lost time.

Perhaps most importantly, Robert F. Kennedy, then a counsel for Senator John McClellan's rackets committee, became convinced that organized crime was one of America's greatest threats. In 1961, he became Attorney General and turned the full force of his enormous abilities and power against organized crime.⁵ The IRS was recruited and Commissioner Mortimer Caplin wrote his staff:

I cannot emphasize too strongly the importance I attach to the success of the Service's contribution to this over-all program . . . The tax returns of major racketeers to be identified by the Department of Justice will be subjected to the "saturation type" investigation, utilizing such manpower on each case as can be efficiently employed. In conducting such investigations, full use will be made of available electronic equipment and other technical aids as well as such investigative techniques as surveillance, undercover work, etc.⁶

Urged strongly by Kennedy to use "technical equipment," the significance of which everyone understood, Hoover intensified tapping and bugging. Although there is a good deal of dispute as to how much Kennedy knew about the microphone bugs, which Hoover justified under a 1954 Herbert Brownell memorandum on internal security, it is undisputed that Hoover engaged in almost as much bugging as tapping. A letter from Assistant Attorney General Miller in May, 1961, reported that the FBI had 67 bugs and some 85 taps in operation as of the date of the testimony; this amounts to some unknown multiple of these for the whole year, since obviously some of these 67 bugs and 85 taps were removed during the year and others installed elsewhere. In 1965, when Attorney General Nicholas deB. Katzenbach tried to force Hoover to terminate these bugs—almost all of which were patently illegal because they generally involved break-ins—Hoover responded that 99% of his organized crime program

involved these bugs and Katzenbach allowed Hoover to phase them out over a six-month period.

Many of these taps and bugs were in for lengthy periods of time—the Maggadino tapes in Buffalo ran to 76,000 pages; the de Cavalcante surveillance lasted four years. Kennedy treated the whole business very casually—he kept no records or review of his authorizations, and the first such effort was made by Ramsey Clark. (Attorneys John Shattuck and Leon Friedman have documented the continuing laxity in the recordkeeping on national security surveillance in their April 24, 1974 congressional testimony.)

We have been told that little of this tapping and bugging was aimed at getting information for specific criminal prosecutions; rather it was gathered primarily for intelligence. That point was made clear by some of the organized crime specialists like G. Robert Blakey, one of the chief draftsmen of what became the 1968 Wiretap Act, who told a congressional committee in 1967:

The normal criminal situation deals with an incident, a murder, a rape, or a robbery, probably committed by one person. The criminal investigation normally moves from the known crime toward the unknown criminal. This is in sharp contrast to the type of procedures you must use in the investigation of organized crime. Here in many situations you have known criminals but unknown crimes.

So it is necessary to subject the known criminals to surveillance, that is, to monitor their activities. It is necessary to identify their criminal and noncriminal associates; it is necessary to identify their areas of operation, both legal and illegal. Strategic intelligence attempts to paint this broad, overall picture of the criminal's activities in order that an investigator can ultimately move in with a specific criminal investigation and prosecution . . . Perhaps the best illustration I can give you is the "airtels" . . . [which] represent the gathering of strategic intelligence against organized crime in that case against Raymond Patriarca.

Tactical intelligence, on the other hand, is illustrated by the *Osborn* case, which the Supreme Court heavily relied upon in the

Berger opinion. You moved in there and monitored only one conversation or only one meeting. You had a limited, tactical purpose, whereas in the Patriarca situation you had a broader purpose . . . So the distinction deals, first, with the purpose of the agency and then perhaps, second, with the extent of time the subject is under surveillance.⁷

Ramsey Clark and others disparaged the value of what was obtained from such "strategic intelligence" techniques. But in the early and middle 1960's few people listened. Organized crime had become the anti-Christ, and Robert Kennedy was leading the Inquisition.

In 1961, Kennedy introduced a bill to permit official wiretapping though he explicitly excluded bugging on the ground that, as Assistant Attorney General Herbert S. Miller put it, the issue "with all its ramifications" needed to be "carefully explored" before legislation was enacted.⁸ Whether this statement was made disingenuously or otherwise, the fact remains that during this period the FBI was operating an enormous number of microphone surveillances.

Pressure for the legitimization of wiretapping came from other sources as well. The President's Crime Commission issued its report in 1967, and near the top of its priorities was organized crime. Influenced heavily by attorneys from Kennedy's Organized Crime Section, the Commission ascribed to organized crime virtually all the ills of the body politic. And while it did not recommend the legitimization of wiretapping—though a majority of the Commission did endorse this—the message was clear. The ABA got on the bandwagon, led by Federal Court of Appeals Judge J. Edward Lumbard, a former prosecutor and the chief judicial proponent of police tapping. Donald Cressey, one of America's leading criminologists, was also converted and wrote angrily, "If organized criminals could be handled as enemies of war, rather than as citizens with the rights of due process, they could have been wiped out long ago."⁹ Apart from the rather cavalier attitude toward guilt, innocence, and the rights of fellow Americans as reflected in Cressey's comment, the fact is that "organized criminals" have been treated as "enemies of war," as Victor Navasky's book makes clear, but with little success in wiping them out.

The pressures were not entirely one-sided however. In the mid-1960's, the enormous amount of illegal electronic surveillance by the FBI, IRS, and others suddenly came to light when an FBI bug was accidentally discovered in a Las Vegas gambler's office and in Washington's Sheraton-Carlton hotel where, as in so many other instances, lawyer-client conversations were overheard. This led to a series of court-ordered revelations of illegal federal surveillance involving some 50 or more cases. (The pattern of accidental discovery of official illegality with respect to wiretapping leading to a loss of prosecutions, which started with the *Coplon* case, has just been repeated in the series of cases culminating in *United States v. Giordano*, where 626 defendants in some 60 cases will automatically go free because of official impropriety.) As a result, President Johnson ordered an end to all electronic surveillance except in national security cases.

At the same time, Senator Edward V. Long began to hold hearings on illegal surveillance by other federal agencies. His investigation discovered, for example, that despite a 1938 Treasury directive banning electronic surveillance, IRS agents tapped and bugged promiscuously, set up some 24 bugged conference rooms, and engaged in breaking and entering—all with an arrogance reflected in the statement of one agent that everything was justified in the battle against criminals.¹⁰ Moreover, the IRS conducted a school in Washington, D.C., to which agents came to learn electronic surveillance and lock-picking and from which experts were sent out to install and remove equipment.

Other agencies were also disclosed to have tapped and bugged widely. One Federal Bureau of Narcotics agent testified that he had broken into homes "hundreds of times" in the 1950's to install microphone surveillances.¹¹ If caught, he reported, his instructions were to deny that he had been authorized to do so by his superiors—even though he had.

The Federal Drug Administration (FDA), the post office, and other federal agencies were similarly exposed. In short, America was presented with a picture of government agents tapping and bugging thousands upon thousands of Americans in knowing and flagrant violation of the law, and often in equally gross violation of constitutional and other privileges—all usually to very little avail. In Kansas

City, Missouri, it was found that a "saturation drive" against organized crime involving 135 agents and at least \$2 million had netted only three convictions, for which the three defendants received sentences of six months, four months, and three months—what Senator Edward V. Long derisively called "minnows."

During these hearings, bugs in martini olives, cigarette packs and other unlikely spots were demonstrated. Shortly thereafter, the President sent up a bill proposed by his Attorney General, Ramsey Clark, to bar virtually all wiretapping.

At this time, in the mid-1960's, the Supreme Court entered the picture decisively and, in the *Berger* and *Katz* cases,¹² set out the contours of a constitutional wiretap statute by approving in principle a gambling wiretap in *Katz*, while striking down the New York wiretap statute in *Berger* as too loose. In the course of its *Katz* decision, the Supreme Court finally overruled the *Olmstead* trespass doctrine. Later, in June, 1968, electronic surveillance was finally legitimated with the passage of Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

The story of the enactment of this legislation has been brilliantly told by Richard Harris in the December 14, 1968 issue of the *New Yorker*. It is enough to say here that, when President Johnson signed the bill legitimating electronic surveillance, Robert Kennedy was dead, but his ghost hovered over the event. It was he who had stimulated the drive against organized crime which fueled the demand for wiretapping, and it was his assassination that propelled the bill out of the House Judiciary Committee where Chairman Celler had hoped to bottle it up. Adding to the irony was the fact that Kennedy had long since lost interest in the organized crime drive and was against the bill. Moreover, the statute was enacted while Ramsey Clark was Attorney General—the only Attorney General since Stone opposed to wiretapping.

These ironies reflected the frailty, if not the impotence, of the liberal tradition in America in a period of crisis. Americans were frightened as rarely before in a time of official peace: they feared street crime, black rebellions, radicals, young people, organized crime. Hanging over everything was Vietnam.

Congress had a pretty good idea of how bad

the bill was. As Richard Harris reported, "all those who voted against it, many of those who voted for it, and most of those who didn't vote at all [believed] the bill was a piece of demagoguery, devised out of malevolence and enacted in hysteria." Nevertheless, records Harris, "in the House, only seventeen members voted against it, and in the Senate only four."

II. WHAT WE HAVE: STATUTORY AND EXECUTIVE AUTHORITY

A. The Statute

Wiretapping and bugging are done under two forms of authority, the second of which has not yet been approved by the Supreme Court: (1) law enforcement surveillance under Title III of the Omnibus Crime Control and Safe Streets Act of 1968,¹³ which requires prior judicial approval; and (2) surveillance for national security purposes which is done upon merely executive approval.

Only law enforcement surveillance is subject to the restrictions (such as they are) of the 1968 Act. And despite the length and complexity of the statute, the restrictions are not very severe. But first, a few words about the facial structure of the Act.

In form, the law bars *all* interceptions of communication except in certain specifically defined classes: (1) if done by law enforcement officials, pursuant to a warrant issued by a court and subject to certain restrictions; (2) eavesdropping with the consent of one of the parties to the conversation; and (3) certain special situations involving telephone company and business monitoring. Illegally-obtained wiretapping is not usable in any official proceeding, and damages for illegal surveillance are possible. States that wish to do so may pass legislation similar to the federal act to allow their police to use electronic surveillance.

The preamble promised that electronic surveillance would be used sparingly and only for serious crimes, and that individual privacy would receive greater protection than before because of the various provisions prohibiting and/or limiting use of the technique, and the provisions of the Act would be enforced.

It hasn't worked out that way.

- Wiretapping has been used very extensively, largely and deliberately for minor offenses like gambling and against small-time operators.

- The conversations of vast numbers of people, many of them totally innocent of any crime, have been overheard—often in surveillances lasting for very long periods of time.

- Few convictions have resulted, and rarely for anything more than gambling and some narcotics cases. Even in some of these cases, there are indications that the wiretap evidence played a minor or negligible role in the prosecution.

- Many of the “protections” of the act have been annulled by judge-shopping, statutory loopholes, and improper execution. There have been almost no successful damage actions to date for illegal wiretapping—though this may change—and very few prosecutions.

On top of all this, we have recently learned of the huge number of Americans eavesdropped upon in the name of national security, without any judicial controls, because President Richard Nixon and Attorney General John Mitchell thought them “dangerous.”

Much of this was predictable and was, in fact, predicted. Indeed, almost all commentators have condemned the act as unconstitutional under *Katz* and *Berger*, but so far, all the appellate courts and all but one district court—and that one was quickly reversed—have found the Act constitutional. Nevertheless, the facial defects of the statute are many. For example:

- It deliberately allows virtually indefinite periods of listening, because it allows extensions, even if nothing is found so long as there is a reasonable excuse for failure to come up with something—even though the *Berger* court condemned 60-day taps as too long.¹⁴

- It draws no distinction between tapping and bugging despite the vastly more pernicious nature of the latter—one can avoid using the phone in many situations, but how does one avoid bugs in one’s home or office? Even Nixon had problems here, even though he authorized the bugs himself. It will be recalled that in the early ’60’s, the proposed bills excluded bugging, but the crime-busters were in command in 1968 and they obviously grabbed everything they could.

- The Act allows judge-shopping without any

limitation. In consequence, only five or six applications for either initial authorization or an extension have been turned down in the six years of the operation of the Act; in New Jersey, for example, the second state most prolific in wiretapping next to New York, a Mercer County judge named Frank Klingfield has never refused an application. In 1972 he issued 134, or one-sixth of the national total. In Erie and Niagara counties in New York—where there are many judges available—one judge issued thirteen out of the fourteen 1971 orders, and in 1970 he issued eight out of nine Erie County orders and all ten Niagara County orders. Many of these have been suppressed in federal and state courts as improperly issued or executed. In Albany County, one judge issued twelve out of fourteen 1971 orders. A similar situation holds true elsewhere, such as in Florida and Baltimore, Maryland.

- The Act is not limited to serious crimes, but allows tapping for a laundry list of federal offenses and an almost open-ended list of state offenses—including gambling, marijuana, and any State offense with a penalty of one year or more.¹⁵

- The Act makes no substantial effort to limit the surveillance to expectedly criminal conversations, but allows a broad definition of what may be intercepted. As a result, there is overwhelming statistical evidence that the bulk of the conversations overheard are innocent. It is not unlikely, moreover, judging by certain individual situations that have come to light, that the statistics in question—which are provided by the prosecutor and therefore can contain all the vices of self-reporting now so well documented from our experience with the FBI’s Uniform Crime Reports—are substantially understated.

These are just some of the facially-obvious problems with the statute. One of the relatively useful provisions in the statute required prosecutors and judges to file reports about the use of Title III wiretaps, and for all the definitional and other shortcomings of this procedure, the statistics tell us some things about the costs and benefits of court-authorized surveillance. Although statistics have been issued for 1968-1973, the 1973 data has not yet been fully analyzed in detail. The figures will therefore be only approximate, but are probably fairly accurate.

**B. The Results as Reflected in the Statistics:
Volume of Surveillance**

In the first place, the statistics document that far from being a rare device to be used only for such serious offenses as homicide, kidnapping and espionage, electronic surveillance has become a routine technique used primarily in gambling cases. Other sources indicate that it is used largely against small-time operators. Indeed, there seems to have been a deliberate campaign against small gamblers named "Project Anvil"; a recent interview with FBI personnel, discussed below, supports this.

The statistics show that in the 1968-1973 period,¹⁶ almost 3,500 taps and bugs were authorized and installed, and almost 160,000 people were reported to have been overheard in more than 2.1

million conversations. Of these, about 48,000 people were overheard on federal taps and bugs authorized by a court order—national security taps *not* included—and some 76,000 on state taps. It is not clear that the state figure includes 76,000 different people, although the federal figure purportedly does try to avoid duplication. The overwhelming proportion of the state tapping was found to be in New York and New Jersey, with most of it in New York. In 1973, for example, New York accounted for 46% of all surveillance and New Jersey for 29%. This is a slight decline from prior years where the two states generally accounted for 80-85% of the total, with New York always accounting for the lion's share.

The following figures tell the story:

AUTHORIZED AND INSTALLED WIRETAPS BY YEAR

Year	Combined Federal and State			
	Orders	Installations	People	Conversations
1968 (6 mos)	174	167	4,250	62,291
1969	302	290	14,656	186,229
1970	597	590	25,812	373,763
1971	816	792	32,509	496,629
1972	855	839	42,182	577,205
1973	<u>866</u>	<u>812</u>	<u>39,788*</u>	<u>495,320*</u>
Totals	3,610	3,490	159,197*	2,131,437*

*These figures are preliminary, in that they are derived from over-all averages reported by the Administrative Office. The exact figures, obtained by analyzing the reports on each individual wiretap and bug, are generally close to these averages.

Perhaps the most troublesome aspect of this massive attack on individual privacy is that, as mentioned before, almost none of it is for serious

crimes like homicide, kidnapping, and espionage, but most of it is for gambling and to a rather lesser extent for drugs. The following table tells that story:

FEDERAL AND STATE ELECTRONIC SURVEILLANCE BY YEAR^a

Year	Gambling	Drugs	Homocide	Kidnap	Other	Total
Federal Installations						
1969	20	4	0	1	5	30
1970	120	39	0	0	21	180
1971	248	21	0	0	12	281
1972	147	35	0	0	23	205
1973	81	28	0	0	21	130
Totals	616	127	0	1	82	826
State Installations						
1968	18	68	20	1	60	167
1969	78	80	19	1	82	260
1970	204	84	20	0	95+7 ^b	410
1971	304	104	18	1	84	511
1972	340	193	33	0	68	634
1973 ^c	365	201	47	2	119	734
Totals	1,309	730	157 ^d	5	508+7 ^b	2,716

^aThese figures are drawn directly from the individual reports appearing in the Appendix to the Report issued by the Administrative Office of the United States Court, submitted to that Office by prosecutors and judges.

^bOffense not indicated.

^cThe 1973 figures are slightly overstated, for they are based on the *authorized* surveillances, which exceeds the number actually installed by a slight amount. It has not yet been possible to determine the exact number of installed state surveillances, for there are certain lacunae in the reports. The differences between authorized and installed are, however, relatively small.

^dThe "homicide" figures are greatly inflated, for they include not just murder, but conspiracy, attempts, threats, solicitations, as well as assaults. Why the latter are lumped in with "murder" is not clear.

Most of this surveillance has gone on for considerable periods of time. Federal eavesdropping has averaged 13.5 days, which is less than the 60 days considered excessive by the Supreme Court in the *Berger* case, but still a high average, given the fact that these instruments are usually in continuous operation every minute of those days. State officials have observed no such time limitations. In 1968, 32 out of 167 state surveillance devices operated for 60 or more days—three for as long as 100 to 199 days. In 1969, over 20 percent operated for 60 or more days, and four transmitted continuously for 200 days. A similar pattern has continued through 1972, when 42 lasted for 60 or more days. Of course, the statute, if one reads it carefully, tacitly permits, and indeed, contemplates such severe intrusions. As noted above, it allows an indefinite number of extensions, *even if nothing fruitful has developed*, so long as there is some explanation for the failure to overhear anything useful.

As a result, from 1968 to 1973 the courts granted 1,323 extensions on about 3,492 installations. The Senate Committee Report accompanying the bill cites, as an example of what the statute allows, a 1955 California case which involved continuous surveillance for over 15 months. (When Senator Hiram Fong pointed out in debate over the bill that it held the possibility of indefinite surveillance, Senator John McClellan, the bill's floor manager, did not deny it.)

Such lengthy continuous surveillance might be barely tolerable if we knew that nothing but criminal activity were being overheard, but such a limitation is practically impossible. Although the statute explicitly requires that investigators minimize the interception of irrelevant, innocent conversations, this is virtually a technical and administrative impossibility, as the reports of wiretapped conversations document. Critics of wiretapping and bugging have stressed the inherently unlimited nature of this technique, and the experience under the Act supports this criticism. More than a few cases have shown that the statutory mandate of minimization has been disregarded by both judges and investigators.

According to the reporting prosecutors' own definition and evaluation, an enormously high percentage of overheard conversations are not "incriminating," whatever the precise definition of that

word. On the state level, for example, the *non-incriminating* conversations that were overheard ranged from 78 percent to 70 percent between 1968 and 1970. In 1971-72, that figure dropped, as the states began to concentrate more on gambling, but the figure still remained near 50 percent. The 1973 figures haven't been calculated yet.

At the federal level, the non-incriminating conversations comprised about 18 percent of the total in 1969, but rose to 40 percent in 1972. Even these figures seem understated, for at least one federal court has found that, although federal prosecutors reported that 85 percent of a group of overheard conversations were incriminating, in fact, only five to ten percent were.¹⁷ More importantly perhaps, once we move away from gambling cases—the proportion of incriminating conversations in gambling cases is necessarily and unusually high because the phones are generally used exclusively for the gambling operation—the proportion of innocent conversations overheard is well over 80 percent.

The large number of wiretap installations for petty gambling in the federal, New York, and New Jersey systems indicates it is not being used sparingly. Moreover, the recent decision by the Supreme Court in *United States v. Giordano*, _____ U.S. _____, (May 13, 1974), indicates that, contrary to Attorney General Mitchell's claims,¹⁸ he never even saw the application to which his approval was initiated.

Moreover, the statutory requirements in §2518(4)(e), that the interception end when the conversations sought are first obtained unless the court orders otherwise, seems to be observed by many judges who simply order routinely "otherwise." Thus, although the Supreme Court seemed to intend that electronic surveillance be subject to more restrictions than a conventional search, the statute provides less.

Finally, it appears clear that the statutory requirement in §2518(3)(c), that the order issue only if normal investigative procedures haven't worked, won't work or are too dangerous, is not being enforced very stringently. Even the one judge hostile to wiretapping held that the burden on the government in this regard is not very great.¹⁹

These factors only point up the frailty of the reed on which individual privacy has been made to

depend—the court order system. With respect to conventional search warrants, judicial supervision is of only limited help, since many judges see themselves merely as the judicial branch of law enforcement operations. Former District Attorney of Philadelphia Arlen Specter, an opponent of law enforcement wiretapping, has put the matter somewhat more delicately;

Judges tend to rely upon the prosecutor . . .

Experience in our criminal courts has shown the prior judicial approval for search and seizure warrants is more a matter of form than of substance in guaranteeing the existence of probable cause to substantiate the need for a search. . . . Some judges have specifically said they do not want to know the reasons for the tap so that they could not be accused later of relaying the information to men suspected of organized crime activities.

So we find wiretapping routinely available to federal and state prosecutors (the latter, of course, only in states with wiretap statutes) who want to spend the money. And it takes a lot of money. The average federal tap in 1973 cost \$12,236 and in prior years, the average cost for a drug case installation was over \$60,000. The state figures purport to be much lower, but are so incomplete and inconsistent as to be worthless. Moreover, even these figures are grossly understated in both the state and federal reports, for they include only the hardware and investigators' and transcribers' time, and omit a very substantial amount of lawyers' and judges' time in preparing and evaluating the applications for permission to tap and bug, to say nothing of the cost of the suppression hearings.

C. The Results: Successful Prosecutions

Measured by the rate of convictions, it is hard to call electronic surveillance much of a success. It is not used very much for anything but gambling, and many of the most important urban states—California, Illinois, Pennsylvania, Michigan, and Ohio—have not even bothered to accept Congress' invitation to allow their police to tap and bug. As of December, 1973, 29 states did not feel this was a worthwhile technique; of those that allow police wiretapping and bugging, five did not even bother to use that authority in 1973.

Moreover, the single most significant wiretapping jurisdiction—the federal establishment—cut its usage from 210 in 1972 to 130 in 1973—a drop of over 35% in one year; this, in turn, followed a drop from 281 in 1971 to 210 in 1972, a drop of 25%, or a drop of over 50% in the two years from 1971-1973. This sharp drop may be attributable to the departure of Attorney General John Mitchell from the Justice Department in early 1972 to operate Committee to Re-elect the President (CREEP), for the drop coincided with that departure. It does indicate that, as some have concluded, electronic surveillance is simply not worth the cost. The official FBI explanation, as reported in an Associated Press story on May 21, 1974, is that the FBI has decided to switch "from quantity to quality," and will henceforth refrain from going after the "mom and pop" bookies who are not directly tied into the crime syndicate."²⁰

The picture as to convictions, purportedly resulting from electronic eavesdropping in those jurisdictions which do wiretap, is still not complete. It apparently takes some 22.5 months to fully process a federal case, so the only reliable results that I have had a chance to analyze fully are for 1969 and 1970. I have, however, made a preliminary survey of the 1971 surveillances and will include that here. Moreover, there is a very difficult question of causality: even where wiretapping was used in a case, how closely related was it to whatever results were achieved? In more than a few cases, courts and prosecutors have commented on the irrelevance of the wiretap evidence. In one state case, the prosecutor himself reported that the conviction was not obtained from the tap. In many cases involving the disclosure of illegal taps, federal prosecutors have argued that whatever wiretapping was done did not produce any of the evidence used at the trial.

Finally, there is the question of appeals and reversals. Many federal convictions will be overturned or are in jeopardy because of the *Giordano* case, and this particularly affects the 1969-70 interceptions, since the Justice Department's procedures were tightened up afterwards.

Even without this rather special set of reservations, the figures still show very thin results indeed.. For 1969-71, only 1,037 persons were convicted as a result of 491 federal wiretaps despite

the expenditure of at least \$4.5 million on the electronic surveillances alone. A more interesting figure is that, of the 210 federal taps installed in 1969-70, only 67, or nearly a third, were related to a conviction. This means that 143 federal installations resulted in little or nothing.

Most of the convictions were for gambling and drugs: of the 1,037 persons convicted, 828 were for those two offenses—643 for gambling and 185 for drugs. More importantly, my check of some of these cases indicates that many, if not most, of these gamblers seem to be small operators, and a recent study provides some support for this conclusion.²¹ FBI Director Hoover opposed the federal anti-gambling law because it dealt with what was essentially “a function of local law enforcement.”²² This concern with “local law enforcement” seems to have reflected a deliberate policy which has now been abandoned as useless.

Gambling is, of course, supposed to be the lifeblood of organized crime, and perhaps these few gambling convictions led to something much bigger. But apparently the FBI has finally decided that things haven't worked out that way. Indeed, most experts are agreed that organized crime, whatever it is, has not been weakened very much.

The arrest figures are, of course, much higher—about 1,400 federal arrests in 1969-70 as opposed to 550 convictions. But the arrest figure is far less significant. For one thing, most arrests do *not* result in convictions. And under the statute, a wiretap order is not authorized unless there is already probable cause to believe that the suspect is committing a crime, which is the same standard that is required for an arrest. In other words, even before the wiretap is installed, there should be enough evidence to arrest someone. It is, therefore, difficult to know how much the tap contributed, if at all, to any arrests. And even with respect to arrests, in 1969-70 over one-third of the federal wiretap installations did not result in an arrest.

The state results are even more meager: 1,597 convictions in the five and one-half years. Again the 1969-70 figures are the most complete,²³ and they tell almost the same story as the federal. For 670 surveillances installed during that period, only 870 people were convicted at a reported cost of about \$1.4 million, with 520, or 60%, in gambling cases, even though gambling accounted for only 282

installations, or about 40%. Drug offenses, probably including marijuana, accounted for another 128. More importantly, only about a third of the installations were related to any convictions.

Not only did 28 states not consider electronic eavesdropping crucial enough to law enforcement to pass the appropriate enabling legislation, but even those that did give their police this authority used it very rarely—except for New York and New Jersey. In 1972, for example, all 19 other states with authorization installed only about 125 taps and bugs out of the 634 total. Perhaps there are reasons other than its lack of utility, but at first blush, it would seem that a crucial investigative device would be employed more often.

Doubts as to the value of wiretapping and bugging come not just from these figures, but from other sources. Many of the Strike Forces created to fight organized crime don't use electronic eavesdropping very much, if at all, as the *New York Times* report on various prosecutors' reaction to the *Giordano* decision indicated. One Strike Force prosecutor told author Edith Lapidus:

It has not often been applicable. We have been able to make a case without it and we have had more indictments and convictions than any Strike Force in the country.²⁴

A New York prosecutor specializing in drug cases told *The Wall Street Journal* that its importance in such cases was greatly overrated. A random survey that I had a student make of major successful prosecutions in corruption, drugs and other areas, as reported in the *New York Times* from July 1, 1972, through June 30, 1973, disclosed very little electronic surveillance in any but a few cases; and, in the few, it was usually consent surveillance involving a wired informer rather than the more conventional wiretapping.

While attorney Henry Petersen of the U.S. Justice Department tried to provide Senator McClellan with data to show the importance of wiretapping and the gambling laws in convicting organized crime leaders, his figures showed mostly indictments only. Very few leaders, and relatively few convictions, related to the wiretaps.²⁵

This lack of utility for crime-solving comes as no surprise, for it flows directly from the fact that wiretapping and bugging are really tools of *strategic*

intelligence, not crime detection. And the payoff on intelligence is, at best, long-term and indirect, and in many instances, very small. Indeed, although one cannot be sure, it does seem as if law enforcement has not been able to get the kind of intelligence that would prevent gangland killings, for example, or head off other unfortunate events.

A type of electronic surveillance that does seem valuable and which I personally find compatible with the Fourth Amendment under proper restrictions is consent surveillance. It seems clear that the use of wired informers is both necessary and helpful; whatever use electronic devices have in extortion and kidnapping cases seems to involve this kind of interception. Moreover, it can be limited with respect to time, space, people, etc. Indeed, all of the cases (except *Olmstead*) in which the Supreme Court sustained wiretapping involved a very precise and limited surveillance, and usually with the consent of one of the parties.²⁶

But such surveillance should not be exempt from Fourth Amendment requirements, as the Supreme Court and the statute have done.²⁷ Consent surveillance is merely a specific instance of the general problems associated with police use of informers. In the past, police have resisted application of Fourth Amendment specificity standards to informers, partly because it is often difficult to specify the individual target—the informer is frequently told simply to infiltrate a group and to learn what he can. This difficulty has generally disappeared when electronic surveillance is introduced, for that is usually done when the police want to zero in on a specific target.

This is not to assert that electronic surveillance is of no value. We know too little to say that, and there probably have been at least a few instances where the information gained from the tap or bug has been very helpful. District Attorney Eugene Gold of Brooklyn, who has become one of the most avid wiretappers, claims to have “broken the back” of organized crime in Brooklyn with the tap in a trailer. Perhaps. So far, little seems to have come from that, but it is still early. Moreover, Gold apparently had Paul Vario, his chief target, on other charges already.

But social policy cannot be decided by a few examples in one way or another. The statistics and

practice of the last six years cast serious doubts on the claims of the tappers, while the danger to liberty and invasions of privacy are indisputable.

III. NATIONAL SECURITY SURVEILLANCE

The statute creates a sharp distinction between court-authorized taps for crime detection and “national security” taps, which have been installed without antecedent judicial approval. In practice, the line has not been that sharp. In the name of national security, FBI Director Hoover installed hundreds of bugs in his fight against organized crime. As reporter Fred Graham has noted, FBI agents apparently had no difficulty justifying (to themselves, at least) a tap on a restaurant on the ground that the Mafia was a threat to “national security.”²⁸

The line became blurred even more when the Nixon Administration claimed authority to tap people whom it considered “dangerous” without any prior judicial approval, and with virtually negligible judicial review if the tap should come to light. In case after case, it ultimately appeared that, under the national security intelligence claim, tapping was done upon people being sought for prosecution, raising suspicions that the national security intelligence cover was being invoked to avoid complying with Title III.²⁹ However, in a startlingly libertarian decision for a unanimous Supreme Court (Justice Rehnquist abstaining), Justice Powell denied the government this authority where *domestic* intelligence was concerned in *United States v. U.S. Dist. Ct.*, 407 U.S. 297 (1972).

The decision has been so widely discussed that there is little need to elaborate on it. But there are a few extremely troubling loopholes in the opinion—very troubling indeed.

The first is that Justice Powell explicitly left open the possibility that a warrant for intelligence surveillance could be obtained under standards more relaxed than normal. Powell declared:

Moreover, we do not hold that the same type of standards and procedures prescribed by Title III are necessarily applicable to this case. We recognize that domestic security surveillance may involve different policy and practical considerations from the surveillance of “ordinary crime.” The gathering of security

intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime.

Given those potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection [quoting *Camara*]. It may be that Congress, for example, would judge that the application and affidavit showing probable cause need not follow the exact requirements of §2518 but should allege other circumstances more appropriate to domestic security cases; that the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court (e.g., the District Court or Court of Appeals for the District of Columbia); and that the time and reporting requirements need not be so strict as those in §2518.

Such a warrant would seem to run directly counter to the long-established requirement of specificity in Fourth Amendment warrants, a requirement that the Supreme Court has said is the essence of the Fourth Amendment.³⁰ Moreover, the distinction between intelligence and prosecution is so thin, as experience demonstrates, that it seems

unworkable. The result can only be a further dilution of Fourth Amendment restrictions in conventional criminal prosecution, which would apply not just to electronic surveillance but to all other investigatory techniques.

Powell was here participating in the current Supreme Court's tendency to allow as "reasonable" every prosecutorial effort to dispense with fundamental Fourth Amendment limitations as to specificity, probable cause and scope of the search. This has been seen in many areas, such as area searches near the border, safekeeping of property, searches incident to arrest, stop and frisk,³¹ and others. Fourth Amendment "reasonableness" is coming to mean little more than that the police come up with some reason, regardless of the Fourth Amendment values and precedents the other way.

Initially, the Justice Department said it would not seek intelligence-seeking authorization of the kind suggested by Justice Powell. But in testimony just a few weeks ago, an FBI spokesman declared that such legislation is being prepared. Hopefully, Congress will reject it. The Fourth Amendment requirements are riddled with so many exceptions already, the standards for probable cause are so loose, judicial scrutiny is likely to be so lax where internal security or suspected violence is alleged, and our experience of abuses from such loose requirements is so bad, that this legislation should get nowhere.

The second loophole was opened by Powell when he explicitly limited the Court's condemnation of warrantless wiretapping to surveillance of *domestic* groups. The kind of link to foreign powers that will make the group not "domestic" is still uncertain. So far, indications are that the Justice Department construes "foreign" very broadly: it has sought to justify surveillance of both the Jewish Defense League and Morton Halperin, both indisputably domestic, as "foreign" surveillance, and it has been upheld by a district court with respect to the former.³²

The volume of governmental electronic surveillance actually affected by the decision therefore remains unclear. The Department stated that it felt required to turn off only six taps, leaving 27 in operation, a surprisingly low figure if one assumes that the various embassy taps were unaffected. Another unsettling note appeared just a few weeks

ago, when David Burnham of the *New York Times* stated that, sometime last August, 82 such taps were in operation, even though President Nixon had said in 1971 that there were to be no more than 50 in operation at any one time. Why the jump to 82 from 27 or even 50?

How much national security wiretapping has occurred in the past is also hard to estimate. Only recently have we obtained any statistics, and these are fragmentary and ambiguous.

In the first place the White House figures, released by Senator Hugh Scott and referred to earlier, show the following "national security wiretaps . . . subject to refinement as the detailed search proceeds."

1945 - 519	1959 - 120
1946 - 346	1960 - 115
1947 - 374	1961 - 140
1948 - 416	1962 - 198
1949 - 471	1963 - 244
1950 - 270	1964 - 260
1951 - 285	1965 - 233
1952 - 285	1966 - 174
1953 - 300	1967 - 113
1954 - 322	1968 - 82
1955 - 214	1969 - 123
1956 - 164	1970 - 102
1957 - 173	1971 - 101
1958 - 166	1972 - 108

(So far, there has been no refinement—the "detailed search" may have been derailed by other "detailed searches.")

These figures are probably understated. Because they refer to "national security wiretaps," it is not clear whether they include bugs. Also, it is most unlikely that they include military, CIA, and whatever local Red Squad surveillance was done on behalf of the FBI, of which there is some evidence. The recent information of 82 in one day in 1973 raises the possibility of a jump to several hundred for the year. Moreover, the figures do not disclose how many people and conversations were overheard.

We do have some information on the latter point from another source. Classified information supplied to Senator Edward Kennedy's staff indicates that from 1968 to 1970, the average

national security tap lasted from 78.3 to 290.7 days. This computation is confirmed by information that has come to light involving the cases of the Jewish Defense League and Morton Halperin. Since the federal taps have averaged about 56 people and 900 conversations per 13.5-day interception, simple arithmetic indicates that each individual federal national security tap caught between 5,500 and 15,000 people per year, and that the 100 annual taps of recent years overheard between 55,000 and 150,000 people per year!

Support for this huge figure comes from a few items of information that have come out of court cases. For example, in the Detroit Weathermen case, it has been reported that one tape contained 12,000 separate conversations, many of them involving lawyer-client conversations.

Except for such episodic disclosures, we have no systematic information as to the scope and extent of such national security surveillance.

The value of this surveillance has been disputed by highly-informed and experienced experts. In congressional testimony this past June, former Attorney General Ramsey Clark declared, "I have tried to estimate—I do not know that it is possible—the value of the [national security] taps that we have. I know that not one percent of the information that we have picked up has any possible use." When Senator Edward M. Kennedy asked, "What would be the impact on our national security if the Executive Branch were to eliminate all warrantless tapping at the present time," Clark replied, "I think the impact would be absolutely zero."³³

Because this security surveillance is carried out secretly and solely by the Executive Branch, it has been completely unregulated. Although a section of the 1970 Organized Crime Act requires disclosure of any surveillance by the Attorney General to the defendant in a judicial proceeding, this provision has been violated by the Department of Justice in many cases including *Ellsberg* and *Kinoy*; the Shattuck-Friedman testimony contains many more examples. Because judges are so reluctant to question federal prosecutors' assertions and representations—although they are getting more sceptical—there doesn't seem to be much that can presently be done about the problem.

There are also indications that this secret

information may be used for improper purposes. For example, in a suit by an Arab-American named Abdeen Jabara, the FBI admitted tapping him and exchanging information about him with Zionist groups. Did this include wiretap information? And, as noted, it seems clear that in many cases, alleged "intelligence" information was actually used to get information for prosecutory purposes.

Much more could be said about national security tapping were there time and space. Its danger is obvious; small as are the protections for court-authorized taps, they are still much greater than are available with the secret and rarely reviewable national security taps. The Shattuck-Friedman testimony shows how feeble are the merely internal restraints, how poor the recordkeeping which makes it even harder to enforce the almost negligible accountability that is now feasible.

The Kissinger tap on the newsmen and governmental aides, the widespread tapping of dissidents (Martin Luther King, Jr. and other blacks) taps on dissenters and on a wide variety of Americans—all have made it clear that "national security" is often a euphemism for personal or political security in an uncomfortable echo of Charles Wilson's "What's good for GM is good for America."

The ideals, on which this country was founded and by which we still purport to live, do not allow us to countenance the kind of claim for unlimited and uncontrolled surveillance that is made in their name, whether for foreign or for domestic purposes. There are bills pending in Congress to try to exercise some control over this wild card in our constitutional deck, and hopefully, the post-Watergate climate will get them passed.

IV. THE WAR MENTALITY

The picture is thus quite clear: wiretapping is of no significant value in crime detection or crime prevention. Its primary value, both understood and intended by its proponents, is as a tool for "strategic intelligence." And even here, the results are sometimes useful, but often worthless, and at a heavy cost.

Yet much more is at stake than simply poor results and heavy expenditures. Not only is the privacy of millions of Americans invaded by these

efforts to obtain "strategic intelligence," but the national attitude toward the social problems that create the dangers, both real and imagined, is distorted and corrupted. "Intelligence" is a weapon of war, and the same mentality that seeks the right to wiretap and bug fellow Americans and others, urges us on to a "war on crime," to destroy the "enemy within." It is the same mentality that uses the weapons of war against political enemies, and that justifies illegality, break-ins, and perhaps even murder against "enemies," as presidential chief domestic adviser John Ehrlichman's testimony before the U.S. Senate Watergate Committee shows. For after all, all's fair in love and war. In hearings before Senator Long's committee, one organized crime-fighter said he would do anything, regardless of legality, to fight organized crime. John Ehrlichman took a similar position with respect to the break-in on Daniel Ellsberg's psychiatrist. And, when narcotics agents terrorized innocent people in drug raids in Collinsville, Illinois, in Massachusetts, and elsewhere, that was justified in the same way—one of the top drug administrators referred to the people involved in drug activities as "vermin" and said, in effect, that everything is OK in the war against drugs. *New York Times*' columnist Tom Wicker drew appropriate parallels in his column on May 4, 1973, when he pointed out that "vermin, gooks, slopes" are all lumped together as "enemies" and subhuman. Collinsville and Cambodia, vermin and Vietnam—all are part of the same military and war-like approach to social problems.

Nor does this stop with "enemies" out there. Those with the war mentality become obsessed with informers and traitors, and surveillance takes place on those in the inner circles. The "enemies" come closer and closer. It became necessary for the Nixon Administration to bug and tap not only radicals and crooks but its own people, including William Safire, the President's speechwriter, who wrote, "in restrained fury," about being tapped. About this tapping he wrote:

'National security,' my eye—during the 37 days in July and August of 1969 that some agent in earphones was illegally (as the Supreme Court later found) listening in to my every word, I was writing the (sh!) President's message and speech on welfare reform.³⁴

And the Watergate hearings disclose further that the President and his top aides were secretly taping their conversations with others and with each other.

It is this frame of mind that seeks to legitimate wiretapping, that talks of "fighting fire with fire," and of winning the war against crime. In this respect, the foreign and domestic uses run together. Prof. David Brion Davis has shown how ready Americans have been to imagine terrifying threats from conspiracies and subversion, and how the reaction has usually been excessive. In a recent review of Dumas Malone's fifth volume on Jefferson, writer Garry Wills noted how a fear of internal enemies who would undermine and destroy the foundations of the Republic, corrupted even so free a spirit as Jefferson in the Burr trial, and how such attitudes led to the notions of "un-Americanism" and the virtual outlawry of what that is supposed to cover.³⁵ The fears that have fed such overreactions have also produced the mentality that recognizes no restraints, that revels in "dirty tricks," and that virtually equates national with personal or political security.

Some of the dangers of such an attitude were discussed almost 40 years ago by Dr. Max Radin, the late noted law educator.

We are invited periodically, in the newspapers, from the pulpit, on the air, to engage in a war on crime. The military metaphor is so persistent and carried out in such detail, that we can scarcely help taking it for granted that somewhere before us, there is an entrenched and hostile force consisting of men we call criminals, whose purpose it is to attack Society, that is to say, us. The matter is presented as a simple enough affair, and it is assumed that if we fight valiantly, we will win and conquer the enemy.

And then? Unfortunately, we are not quite clear what is to happen then.

Last year Dean Francis A. Allen of the University of Michigan Law School wrote:

Wars are attended by certain inconveniences, and one of these is a war psychology which, with only slight encouragement from circumstances or special

pleading, can be quickly converted into a war psychosis. A society in such a mental state is not likely to achieve an accurate grasp of reality, to establish sensible priorities, or to make correct calculations of social costs involved in policy alternatives. Evidences of these distorted perceptions abound in contemporary statements about law enforcement. Thus one frequently encounters the reflex of politicians and law enforcement spokesmen that attributes disturbing criminal occurrences to nation-wide conspiracies (usually of a radical cast) or to the efforts of 'outside agitators.' Few of these assertions are ever confirmed by competent evidence.

The issue, of course, goes beyond the matter of law enforcement efficiency. One who elects to launch a war on crime should be aware that he is electing to engage in civil war.³⁶

And Professor Leslie T. Wilkins has noted that the result of such thinking is evasion of the real problems by personifying them, by thinking that by catching some criminals—and these can never be more than a small percentage of law-breakers—we have contributed to a significant reduction in a crime.

All these dangers will be compounded by new technology, as surveillance devices, developed for the CIA and others for use in Vietnam against foreign enemies, are transferred to civilian life in the battle against domestic enemies.

In this nation, we have a history of fear of conspiracy, of foreign influences, a fear that has frequently produced great repression for little cause. Wiretapping is an essential element of this repression; it seeks to reach into the mind and thoughts of "the enemy within." It has little or no place in a free society and luckily there is no great need for it.

V. SOME PROPOSALS

Outright repeal of the legislation legitimating electronic surveillance is the only sensible approach. However, if that is not politically feasible, the following amendments may do some little good:

1. Ban state wiretapping. The results are very

meager; the abuses, such as judge-shopping and lengthy surveillance, are very great; and there is little basis for allowing it to continue. If allowed at all, limit the authority to tap to murder and kidnapping, carefully and properly defined.

2. The federal authority should be limited to murder, kidnapping and espionage. Congress should insist that wiretapping and bugging are not routine investigative techniques to be used for gambling and drug cases, but are dangerous devices that can be allowed only for the gravest of threats.

3. Lengthy, continuous surveillance should not be permitted. Extensions should not be granted except in rare cases. There should be a maximum of five days for any surveillance unless it is absolutely clear to a court that one additional five-day extension is necessary. Moreover, the type of conversation to be intercepted should be specifically described: the parties thereto, the subject matter, the time when it will take place. The practice of listening in on hundreds of conversations in order to catch a few that are "incriminating" must end. If it cannot, then electronic surveillance is so clearly incompatible with the Fourth Amendment that it should be prohibited entirely.

4. Room or house bugging should be prohibited. A significant number of surveillances (five percent in 1972) are of this variety, and it is especially indiscriminate. One can perhaps refrain from using a telephone, but with a room bug in the home or office, there is truly no place to be free from the "big ear." The draftsmen of the statute ignored this difference between tapping a telephone and bugging a room or a house, and ran them together, probably quite deliberately.

5. Notice must be made available to *all* people who are identifiable as having been overheard.

6. Challenging a tap or bug should be available to anyone against whom evidence obtained from the surveillance is to be used, either directly or indirectly.

7. Damages should be available against the

government for improperly authorized surveillance, except where the eavesdropper acted on his own.

8. A Study Commission has been established pursuant to the Act. It should not contain any members appointed by the Executive Branch, since it is that Branch whose acts are being evaluated. Eight members should be appointed by the majority party leaders in the House and Senate and six by the minority party leaders, with a Chairman to be chosen by the Chief Justice.

9. A joint congressional committee should be established to oversee all national security surveillance. It should obtain a detailed annual report from all agencies of the Executive Branch engaging in such surveillance and should issue a public report of the non-classified material. If national security intelligence surveillance is to be permitted, it should only be pursuant to a court order, and should be very narrowly confined.

Wiretapping and bugging are "dirty business" and it is now clear that they do not help to solve or even prevent much crime. They are expensive, time-consuming, and gravely threaten a free society. The Act should be repealed, and we should return to the flat ban of former §605, with some strengthening of the provisions for damages and other enforcement devices against such practices. If that is not politically feasible, then we should try to impose some limits on these pernicious practices that would at least bring them within hailing distance of the Bill of Rights. Perhaps the Watergate disclosures and their fallout will awaken the nation to the grave dangers it faces from "men of zeal," who often are not "well-intentioned," and are certainly "without understanding."³⁷

Notes to REFLECTIONS ON SIX YEARS OF
LEGITIMATED ELECTRONIC SURVEILLANCE

by Herman Schwartz

1. *New York Times*, February 2, 1974.
2. *New York Times*, May 9, 1974, p. 43, col. 7.
3. *Olmstead v. United States*, 277 U.S. 438 (1927).
4. Informal authority to gather intelligence against Fascist and Communist threats was first given to J. Edgar Hoover by President Franklin D. Roosevelt in 1936. See John Elliff, *Crime, Dissent and the Attorney General*, 154 (1971).
5. The story is told vividly and thoroughly in Victor Navasky's *Kennedy Justice* (1971) and the next few paragraphs draw on that.
6. *Kennedy Justice*, p. 49.
7. Hearings on Controlling Crime through More Effective Law Enforcement Before the Subcommittee on Criminal Laws and Procedures of the Senate Judiciary Committee, 90th Cong., 1st Sess., 957-58 (1957).
8. *Kennedy Justice*, p. 78.
9. See President's Commission on Law Enforcement and Administration of Justice, *Task Force: Organized Crime*, p. 29 (1967).
10. Hearings on Invasions of Privacy Before the Subcommittee on Administrative Practices and Procedures of the Senate Judiciary Committee, 89th Cong., 2d Sess., 1252-53. (1966).
11. *Id.* at 1954.
12. *Berger v. New York*, 388 U.S. 41 (1967); *Katz v. United States*, 389 U.S. 347 (1967).
13. 18 U.S.C. §2500 ff.
14. 18 U.S.C. §2518(1) (f).
15. 18 U.S.C. §2516(1), (2).
16. A rather elaborate analysis of the statistics and related material for 1968-71, some of which is summarized here, appears in my ACLU Report, *The Costs and Benefits of Electronic Surveillance* (1973).
17. *United States v. King*, 335 F. Supp. 523, 542-43 (S.D. Cal. 1971).
18. Elliff, *op. cit.*, p. 68.
19. *United States v. Whitaker*, 343 F. Supp. 358 (E.D. Pa. 1972), *rev'd*, 474 F. 2d 1246, (3d Cir. 1973).
20. *Buffalo Evening News*, May 21, 1974, P. 17, col. 2.
21. Edith Lapidus, *Eavesdropping on Trial*, 161 (1974).
22. *Id.* at 68.
23. There are almost no reports for the 1968 installations.
24. *Id.* at 162.
25. See 118 Cong. Rec. S11159 (daily ed. July 24, 1972). The correspondence is examined in detail in my 1973 ACLU Report at 84-85.
26. The cases are discussed in H. Schwartz, *The Legitimation of Electronic Eavesdropping: The Politics of "Law and Order,"* 67 Mich. L. Rev. 455, 464 (1969).
27. *United States v. White*, 401 U.S. 745 (1971).
28. Fred Graham, *The Due Process Revolution*, 273 (1970).
29. This includes the Ellsberg, Harrisburg, Leslie Bacon, Detroit Weathermen, Jewish Defense League and Chicago Conspiracy cases, and many other cases. The list is collected in the Shattuck-Friedman testimony cited earlier.
30. *Berger v. New York*, 388 U.S. 41, 55-56 (1967).
31. *Almeida-Sanchez v. United States*, 93 S. Ct. 2535 (1973); *Cady v. Dombrowski*, 93 S. Ct. 2523 (1973); *United States v. Robinson*, 94 S. Ct. 467 (1973); *Adams v. Williams*, 407 U.S. 143 (1972).
32. *Zweibon v. Mitchell*, 363 F. Supp. 936 (D.D.C. 1973), appeal pending.
33. This and the Justice Department testimony appeared in Hearings on Warrantless Wiretapping Before the Senate Subcommittee on Administrative Practices and Procedures of the Senate Judiciary Committee, 92 Cong., 2d Sess., 53 (Clark), 18 (Justice) (1972).
34. *New York Times*, August 9, 1973.
35. Garry Wills, *An Un-American Politician*, *New York Review of Books*, May 16, 1974, pp. 9, 11-12.
36. Allen, *Reflections on the Trials of Our Time* (Holmes Lecture 3/15/73). The Radin quote is from Dean Allen's Lecture.
37. The quoted words are from Brandeis' well-known warning in his *Olmstead* dissent about "men of zeal, well-meaning but without understanding." 277 U.S. at 479.

Hearing, Wednesday, June 25, 1975

Washington, D.C.

The hearing was convened at 9:35 a.m., in Room 6202, Dirksen Building, William H. Erickson, Chairman, presiding. Commission members present: William H. Erickson, Chairman; Richard R. Andersen, G. Robert Blakey, M. Caldwell Butler, Florence P. Shientag.

Staff present: Kenneth J. Hodson, Esq., Executive Director; Michael Hershman, Esq.

PROCEEDINGS

CHAIRMAN ERICKSON: Ladies and gentlemen, this meeting of the National Wiretapping Commission is now called to order.

We have a very tight schedule, and for that reason, as we proceed we are going to try to stay within the confines of the schedule that we have set.

Before covering the matters that we will go into today, I would like to suggest to all of the witnesses that are here today that where opening statements are to be used, we will appreciate each witness tendering to the reporter the opening statement with the thought that that statement will be included in its entirety within the record of this proceeding.

But for the sake of brevity, in order to keep this meeting within the time frame that we have, we would appreciate each witness attempting to summarize that opening statement in his own way within a period of five minutes and then, of course, the questioning will proceed by the staff in order to develop the areas upon which each of you has been asked to testify as experts in the field.

When Title III of the Omnibus Crime Control and Safe Streets Act, the so-called Federal Wiretap, was enacted, its proponents acknowledged a well-known fact: Section 605 of the Federal Communications Act provided practically no deterrent to the use by police and by private individuals of telephone taps and room bugs.

In drafting Title III, they provided severe penalties, \$10,000 and five years in jail as the penalty for violation, and also provided for the confiscation of the equipment, liability for civil damages for all wiretapping electronic surveillance, except that which was specifically permitted by the Act.

It was believed that this approach would stamp out illegal eavesdropping but would permit the use of wiretaps and bugs under carefully restricted cir-

cumstances such as for law enforcement and with the consent of one party or with the approval of the court or by the telephone company to check on the adequacy of its service.

The hearings conducted by the Commission in the past have dealt mainly with wiretapping and electronic surveillance as related to law enforcement, with emphasis on the problems involved in obtaining and executing court-authorized wiretaps.

During the next three days of hearings we shall be discussing illegal wiretapping as it affects the general public, covering such areas as industrial espionage and use of electronic surveillance by private investigators.

We will also hear about the monitoring of telephone calls by the telephone company.

We will hear testimony from people who have knowledge of and experience with illegal wiretapping and bugging and with the manufacture and use of electronic surveillance devices.

We hope to present to the Commission and to the public valuable information of the nature and scope of illegal wiretapping activities in the United States today.

We will begin by hearing from manufacturers of electronic surveillance equipment regarding the impact of Title III provisions on their sales and selling procedures. We shall then hear from a convicted private investigator, have a display and demonstration of electronic surveillance equipment, and hear from three witnesses who have been concerned with instances of illegal police wiretapping.

Tomorrow we shall open the testimony on a case of illegal political wiretapping and hear from witnesses on the potential and extent of industrial espionage and then present panels of representatives of companies offering counter-measure or debugging services and equipment.

Friday we will hear from a representative of the Department of Justice who will discuss enforcement policy regarding Title III violations.

Then we will close the hearings with testimony from three witnesses on telephone fraud and telephone company monitoring and a discussion of pre-1968 electronic surveillance in organized crime.

Since we expect to hear from a total of 22 witnesses in only three days, we ask that questions be confined to the suggested relevant areas of inquiry for each topic.

We open our hearings today with a three-member panel of manufacturers of surveillance equipment.

First we welcome Mr. Andy Bower of Bell & Howell.

Next we have Jack N. Holcomb, president of Audio Intelligence Devices, one of the leading manufacturers of electronic equipment, from what I understand. And Mr. Holcomb, I believe, has the background of having worked in this field for more than 25 years.

The third member of the panel is Mr. Michael Morrissey, formerly associated with B. R. Fox, Inc., a small company which developed electronic surveillance techniques and devices before it was dissolved in late 1974.

Mr. Bower, I understand Bell & Howell is represented by counsel. Will counsel please identify himself for the record.

MR. DORSEN: My name is David M. Dorsen, from Washington, D.C.

CHAIRMAN ERICKSON: Mr. Dorsen, do you intend to participate in any of the questions by answering or offering advice?

MR. DORSEN: No, Mr. Chairman, I think Mr. Bower is the witness and will be happy to answer all your questions.

CHAIRMAN ERICKSON: All right.

Will you gentlemen kindly stand and be sworn.

[Whereupon, A.T. Bower, Jack N. Holcomb, and Michael Morrissey were duly sworn by the Chairman.]

MR. HODSON: Mr. Chairman, before the witnesses begin to testify, in order to expedite the proceedings, I would like at this time to suggest to the Commission that all opening statements, all our staff reports, and all staff exhibits be entered into the record.

CHAIRMAN ERICKSON: Is there any objection?

Hearing none, it is so ordered.

[The documents referred to follow.]

VIEW FROM THE BASEMENT

[Note: Names of persons and places in this account have been changed to protect the "personal health" of the man known as George Nantes.]

George Nantes has given the Commission a rare and valuable glimpse into a basement operator's world. This May he spent a day with some of our staff talking about the origins, techniques, business associations and ethics of his career as a self-taught manufacturer (and occasional installer) of electronic eavesdropping equipment.

Nantes is a man of the street. He is also a professional. His craftsmanship rivals that of the big electronics firms and his ethics reflect those of the straight business world.

Nantes was born in 1928. He grew up in the Pacific Northwest. His father, a second-generation Bolivian, had mar-

ried a Bolivian woman and led a marginal life as a restaurateur and dealer in exports-imports. At an early age Nantes began tinkering with electric gadgetry. He built his first crystal set at 12 and his first marketable radio at 13. He left high school in 1944 to attend an RCA electronics institute—bribing its director with a gift of foreign postage stamps so his age wouldn't be held against him. During the last years of World War II he built radios and hawked them to sailors.

He joined the Army in 1947. Angered by a racial slur from a sergeant, he went AWOL, turned himself in 10 months later, spent a year in stockade, and left the Army on a bad conduct discharge.

For the next 18 years Nantes skipped through a series of electronics jobs: TV repairs, technical writing, radio transmission work, more TV repairs. He earned between \$100 and \$300 a week and from time to time set up his own TV repair business. Most of the time, though, he worked for others.

He recalls one employer of the early 1950s with enthusiasm: "The boss took us to a whorehouse every morning before work. He brought girls over during business hours, too. We sure worked hard for that guy."

Midway through this period Nantes got married. "What a mistake *that* was," he says. He left home after two years, went to sea as a merchantman, and occasionally sent his wife money "to pay her booze bill." When he returned after six months he found his wife had "scored" with his business partner and forced him, Nantes, out of his own company. Apparently they did this with his mother's help.

"After that I was in a real depressed state," he says. "I took up with a girl who was an addict and she turned me on to heroin for five or six years, 1959 to 1964. I supported the habit by stealing and robbing, and they busted me a dozen times or so. Usually I got a suspended sentence, but the last time they sent me to jail. I did 10 months there. I just sat around and cold-turkeyed it, cleaned myself up from the H. and it was then that I first got to know the police."

A year after his release Nantes married again—a "nice" girl whose father had worked for Roosevelt's European recovery program. He set up his own TV repair firm, handpicking a wealthy clientele and earning a little over \$300 a week. This business lasted until he got hooked by the lure of bigger money in electronic surveillance.

Today Nantes is still married but he has also taken up with the wife (now divorced) of a well-known novelist. "I divide my time in half," he says. "Now and then one woman yells about the other, but I just dismiss it from my mind. My wife is not very earthy, not sexually attuned. She floats through life. The other one screams and hates my wife and threatens to kill me if I don't divorce her."

"I do what I want. They're all creatures of emotion. In a crisis women break down, cry and sob. They aren't bright enough to work with me on bugs. My wife says what I'm doing is right because it slows down the drug traffic. The other one says, 'Wow, your life sure is exciting!' I say, 'Come on down to my basement and see just how exciting it is.'"

How did Nantes come to lay out his story for us? He stepped across the threshold of the law once too often. Two years ago a man named Clive, who said he was a private investigator, bought some bugging equipment from Nantes. Clive then introduced a colleague from New York named Pedro. Later, on the phone, Nantes made the mistake of selling Clive some bugs for delivery to Pedro in New York. This was an illegal transaction under Title III Federal Wiretap Act. Soon afterwards Nantes was drinking coffee in his room when Clive and Pedro came in with a half-dozen other men. Clive said he was with the U.S. Attorney's office, Pedro said he was with the DEA, and the others said they were with two or three different law enforcement agencies. They invited Nantes downtown.

"They had me cold," he said. I figured I hadn't done anything wrong and could beat it in court, but I didn't want to lay out the money. So I talked to them. I gave them a few cases."

The cases, which involved *mafiosi*, are still pending. Although he was forced to testify, Nantes found he liked it. He is still an informant today. "I don't owe the law a thing," he says, "but I enjoy wising them up. They told me it would endanger my personal health. Well, I'm not constituted to have a quiet life."

With a guarantee of anonymity, Nantes agreed to talk with us. We asked him why he wanted to do it. "Oh, I don't have any heart-throbbing motivation," he said. "You guys might even revise the law in a way that hurts me, but I'll still tell you things other guys wouldn't. It breaks up my week."

Working With the Narcotics Squad

Nantes showed up for the interview wearing beltless navy blue trousers, a half-mod blue jacket and a flowery blue sports shirt open at the neck. He chain-smoked through seven hours of conversation.

After talking about his early life he told us how he became a basement operator in 1967. A girl who lived across the street from his apartment introduced him to an out-of-state policeman working for a county prosecutor's office. They talked about bugs, and the policeman showed Nantes X-rays of equipment designed by a well-known basement operator, Zebra. Nantes' curiosity got the best of him. Promised a big payment, he set to work making bugs for the policeman.

"The X-rays were too crude to help," he says. "I spent many sleepless nights working out my own design. Finally, after three months, I developed a free-running oscillator with an audio amplifier. It was a little over an inch in diameter, ran off a nine-volt battery for about 30 hours, and transmitted at 115 megahertz. I'd never seen another bug or schematic before, just invented my own."

The out-of-state policeman never paid up, so Nantes contacted one of the detectives who had arrested him for drug possession. The detective brought along his boss, Sergeant Harry Whorton, and soon after that Nantes was selling \$25 bugs to Whorton's special narcotics unit on a more or less regular basis.

"The narc unit was my bread and butter for nearly two years," Nantes says. "Little by little all the cops in the unit came knocking on my door. I sold them \$25 room bugs that cost \$6.00 to build. After a while I studied Zebra's bugs real well, and some of Jim Zayres', and some of Century's. Mine were the best. They wiped out all the rest. And so I progressed into phone bugs, the same oscillators with a trigger switch. Ninety-nine percent of my business came from the narc unit and other city police. I raised my price to \$100 for a device that took me 20 minutes to make. The components could have gone into anything—TVs, radios. They were easy to get. The capacitors and transmitters came from Mouser Corp. in California, the mikes from Tibbeths in Maine, that's just about it."

One day the cops asked me to install a telephone device. I did. During 1969 and 1970 I put in lots of phone bugs, taps and a few room bugs for the narc unit. They never mentioned court orders. I figured that was their business. Later I learned they had no court orders, but I never asked them if they were doing illegals.

"I must have done a half-dozen wiretaps for the narc unit from 1968 to early 1970, and I sold them about \$10,000 worth of equipment. They usually paid cash up front. Only once did I take a cop's personal check, but I took quite a few checks from the unit itself. They kept coming back for more even after they had a whole shitload of the stuff. They said it was hard to get to. This was after 1968. It was like Title III never happened."

"One night Danny Alvaroa of the narc unit came to my place. They always wanted things done at inopportune times. Alvaroa took me downtown to a plant they'd set up in a basement. They'd forced the apartment superintendent to let them use the room after they caught him making it with some broad—getting fellated, you might say."

"The tap they'd put in wasn't working. I fixed the wiring in 10 minutes and went home. The next morning Alvaroa woke me up and said, 'We've got them!' Using information from the wire, they'd picked up about 100 kilos of H from Argentina. Later it turned out that they'd pocketed some of the money but arrested the dealers anyway."

Nantes' work with the narcotics unit gave him a cynical view of police behavior. "Nearly every narc guy I dealt with is in jail now or heading there," he says. "That's 30 or 40 of them. Wharton is in jail. Alvaroa is in jail. Two other guys have killed themselves." Nantes' business associates were convicted on charges of illegal wiretapping and shaking down suspects.

"Cops are human," he says. "They smoke marijuana like anyone else. I've often seen them high at my place. And they turn their back on crimes their informants commit."

"If a cop earning \$15,000 to \$20,000 gets offered a bribe worth 10 years' salary, he'll take it for sure. Why should he be different from the rest of us, even with the oath he takes? But cops do have a mentality of their own. You ask them why they steal money from a dope dealer and they say it's "dirty" money. If they shake down a whore or a bookie, who are they hurting? Police departments are closed corporations. Sons learn from their fathers. They think they're fighting crime when they steal money from a bookie."

Installing Illegal

Through Whorton, Nantes met two private detectives named Rooney and Cummings. They were ex-cops, and Nantes calls them "slimy." Nevertheless he did business with them for several years. Rooney looked like Dick Tracy and Cummings looked like Tracy's sidekick Pat Patten.

On his first wire job for the two private eyes in 1968, (after Title III) Nantes posed as a telephone repairman. Someone in the building spotted him, demanded his identification, and said, "I didn't know Bolivians worked on telephones." "Oh," replied Nantes, "there's more of us all the time." The phone he was supposed to tap was out of order, so Rooney and Cummings refused to pay him.

Nantes got even by installing a defective drop-in mike in the house of an old woman whose son had reportedly embezzled several million dollars. Rooney and Cummings paid Nantes \$300 for the bug, and Rooney sat around for a couple of days without hearing a thing. Finally, by chance, he saw the suspect entering the house. He tailed him to the Bahamas, then offered Nantes \$500 to drug the man and bring him back. Nantes refused.

Another time, Rooney and Cummings had Nantes bug the phone of a dispatcher in a big warehouse. "The two dimwits tripped a police alarm and I found myself staring into a 38 revolver," Nantes says. "I acted like Cummings was my boss and we were working late at the warehouse. When Cummings played his part okay, the cops left. We bugged the phone at the request of the foreman and put a tape recorder in his office. The foreman never caught the dispatcher doing anything wrong. One day he called me, though, to say he was depressed by all the bad things he overheard his men saying about him in the dispatcher's office."

The only other non-police job Nantes told us about had to do with a bandleader whose wife was "screwing everybody in the neighborhood." The bandleader asked a telephone repairman to bug his wife's bedroom, the repairman introduced him to Nantes, and Nantes brought his two shifty colleagues into the case. For \$2,000 Nantes bugged the bedroom.

"It was a bad job," he says. "The problem with illegals is you can't handle the accidental crap—in this case it was a radio station lobe (signal) that interfered with my transmitter. For \$50 I hired a junkie to yank out the bug. He got caught by the landlady and swallowed it. I said, 'Don't give me any sad story, vomit it up.' He did, wire and all."

Nantes has sold his hardware to a few private businesses, but not often and not in large lots. He has also done a dozen or so debugging jobs. "I never found anything," he says. "I charge \$500 a phone and \$200 a room. I don't really want to do this kind of work so I charge what the traffic will bear.

Nantes is a sports car buff. He owns an Alfa-Romeo, a Spider and a Mercedes 6.3 with a "super engine." As a buff he got to know Ralph Fields, the owner of a high-class imported car salon. One day Fields called him up and said a friend of his, Severina Dufy, wanted her apartment debugged. "I went over there and the doorman checked me out real good," Nantes recalls. "Upstairs I knocked, the door opened, and this naked girl took me by the hand to a sofa and started kissing me. She jumped on my lap. What do you charge?" she said. I said \$500. "Will you take it in trade?" I said no ma'am, I want cash. "What's the matter, don't you like me?" Sure, I said, I'll give you \$10 off. She threw me out of the apartment."

"Next week Fields called again and sent me to debug another whore, Justine D'Arcy. The door opened and she was naked, too, 6'3" tall, in her early 40s, no eyebrows. Same thing happened. Fields wasn't doing me any favors! Later I learned the Dufy broad *had* been bugged. They found the transmitter but nothing came of it, no indictments. Somebody must have made a deal."

Going Interstate

Nantes' income suffered a heavy blow when the narcotics unit was broken up. "It took lots of money out of circulation," he says. "The few guys who weren't put away were leary of me. They even crossed the street when they saw me coming. Fortunately, about that time I started branching out. I went interstate. An ex-FBI agent introduced me to a retired cop who was working with a sheriff's office in Florida. When I met the sheriff we closed a deal for \$10,000 worth of equipment. His office bought pocket transmitters, slave units, harmonica bugs, tape recorders, series and parallel wires, drop-in mikes, the works.

"Believe me, I didn't make a thing. The sheriff took me into his office and asked what was in it for *him*. I had to give the bastard \$1,000 worth of tape recorders, telephone bugs, a radio and an attaché case. Boy, was he greedy! His officers wanted money, but I gave them some equipment and took them out drinking. I blew \$300 in booze, and then they wanted me to go out and help them beat up queers.

Three weeks later, when he was driving the equipment to Florida, Nantes smashed up his \$10,000 BMW-2800 and got a bad whiplash. His first interstate deal was practically a washout, but it broke his dependence on local police. Today, through a Atlanta distributor named Peter Andrew Wren, he is marketing his hardware all over the country.

"Peter gets my stuff at 50 to 60 percent off," Nantes says. "He wants me to go into full-time business with him—he'd get all my stuff at cost and split the profits. It would keep me off the road. For some reason Peter likes to travel, but I'd rather stay home and mess around the garden, or hunt, or go fishing. I'm considering his offer. Meanwhile, he's doing okay—sold \$50,000 worth of stuff a year for me when business was good. It's down now. The recession did it.

"I really hate to watch nickels and dimes, but it's come to that. If you guys require licensing I might have to get out of this work altogether. Maybe I'd go back into TV repairs, open a store and hire young guys to do the heavy work. This bugging business may be coming to an end, but I sure don't want to haul TV sets around."

Was it the recession or the anti-wiretapping mood of the country after Watergate that hurt business? "Nah, it's the recession," says Nantes. "The other thing didn't make all that much difference. By the way, the Watergate equipment was very poor—just an oscillator, that's all. If they'd used my stuff it would have worked the first time and Nixon would still be Pre-

sident. You see, I'm well-known in the wrong circles. If the Watergate people had come to me I'd have sold good stuff to them."

Talking Shop

Nantes' criticism of the Watergate operation led to a conversation about the techniques, folkways and personalities of his trade.

"I don't meet too many other basement operators," he says. "There are five or six of them in this part of the country. Once I went down to visit Zebra and he threw me out of his office. He thought I was trying to steal his circuitry. Some people in this business are cop-buffs. Peter is. He likes the intrigue. Zebra hates cops. Me, I'm a money buff."

"Guys like me and Zebra don't go to these big security conventions. That's for the name manufacturers. The big guys don't like me, but whatever they do I can do better.

"Electronics work is fun. Someone tells you Bell & Howell has just turned out a good item, you go and work on it and after a few days you come up with something even better."

"My test equipment is really good. I have spectrum analyzers, Hewlett-Packard stuff, Techtronics, Singer and so on. It's better than Zebra's or Stoneman's. It has more power than Bell & Howell's or Holcomb's, though the last two use crystal control which is more stable than mine and more expensive. If business warrants it, I'll give them crystal control. That would knock the piss out of Bell & Howell and Holcomb. Besides, when a Bell & Howell unit breaks down it takes you four weeks to get a new one. I can make replacements right away."

"Since 1965 there hasn't been much change in the technology. Miniaturization is about the same. How much smaller can you get? Oh, the independents are putting out a few new devices, but we haven't had much R&D since Title III because there's no incentive for it. The same is true of counter-technology. Some of it may look different, it may be just a little bit more sensitive, but really it's the same old stuff."

What devices are made primarily for law enforcement? "Oh, any room bug, any telephone bug. A room bug has more audio gain, or reach, than a body transmitter. To be honest, it's what you *call* the goddam thing. I can take my body transmitter and use it as a room bug. On out-of-state orders, though, I make the distinction: I won't sell bugs."

"Most of the techniques I used on installations were simple. On wires I'd call the number I wanted to tap on a handset, then lay a pair of pliers across the terminal pairs. When I hit the right one the ringing would stop with a *click*."

"Lots of people think you can hear something funny when your phone is tapped. That's not true. On a parallel wire you can't hear a thing. Even on a series wire, where the audio drops about six decibels, it's *consistently* lower so you don't notice. A competent wire just can't be detected."

"There's a fair amount of bullshit in this business, especially in the counter-measure area. Once a guy asked me to make him an "all-bug defeater." He gave me \$1,000 for it. I called up Abe Brumwitz and told him to make me something for a fast hundred bucks. I told him to throw in a few relays, lots of wiring, male and female jacks, a 100-watt lightbulb—in other words, to make it look real fancy. We sold it and got no complaint. Later a well-known counter-measure guy began selling the same item for \$1,000 all over town. This debugging stuff today is mostly bullshit."

"I've done a few special jobs I've really enjoyed. The police in Florida wanted to find out if two guys knew each other, so I wired their phones together on the same tap. I said, 'call them up at the same time, and if they show recognition when they pick up, they know each other.' It worked. The sheriff still has my device on his wall."

"Another time the police got into a jam trying to bug a guy whose security was too good. They couldn't get into his place.

So I hid the bug in a nice-looking lamp. The police set the lamp near the guy's door. Sure enough he stole it and brought it into his room, and after that they heard everything he said."

Basement Ethics

"I know several manufacturers that deal illegally. They sell to the Gambinos and other *mafiosi*. I never took a clear step into illegal work myself, except for the warehouse and bandleader bugs. But I *told* you about them!"

"I try to operate under Title III. No more stuff to private investigators. I'll sell to police if they identify themselves. I just make a product; they can do what they want with it."

—What about the time you got tripped up by Clive and Pedro? we asked Nantes.

"I figured if Clive took the stuff to New York it was his business, not mine," Nantes said. "I didn't do anything wrong."

—But the federal law, Title III, says you can sell only to law enforcement.

"Well, that's your interpretation. There was money up front. I don't think I was breaking any law."

—You can't buy a component today that hasn't been sent through the mail. They all go through the mail. So if the component ends up in a surveillance device and you sell it to Peter Andrew Wren, you're violating Title III.

"Mmmm . . ."

—And Title III also says you can't stockpile devices.

"That's unfair! You're telling me how to run my business. How can you meet an order without an inventory? I stockpile!"

—When your distributor calls in an order, how do you know he's selling the stuff legally?

"You *don't* know. You go by faith."

—How would you rewrite Title III to do away with illegal sales?

"I'd put strict controls on manufacturers, serialize every piece of equipment and file the number with the government. But any government guy will turn his head for enough money. How do you stop that?"

—With 10 years' jail and a \$5,000 fine, maybe.

"Only if you can enforce it. How many busts against illegals have you heard of? Not many. There's a helluva lot of illegal wiretapping going on. It's the money! The rewards are greater than the risks. Before 1970, when I was broke, I'd install bugs and wires. Now I don't do it because I don't need to."

—What would it take to get you back into illegals?

"Money. If a guy offered me \$50,000 I'd think about it and then do it, but I wouldn't do it if the risk was high and I wouldn't do it for less. If I got caught on a \$25,000 job the money would all go to a lawyer. No thanks!"

—Even if it was a really beautiful job?

"There *are* no beautiful jobs."

—What if you're short of cash?

"That's another story. I'd take less."

—Suppose someone wanted a bug or wire job done real bad but didn't have the kind of money you wanted?

"I'd send him to some of my enemies to make havoc for them. I can think of four or five guys who'd do it despite the threat of a fine or jail. You just can't enforce against illegals with the present law and the present type of law enforcement. If you get a college kid or TV repairman, he'll tap for very little. I'll make you a bet that out of 100 TV repairmen 40 would install a wire or bug. The same goes for radio men, telephone men. Any competent technician can do a hard tap—and \$1,000 is a month's pay. If you offered them \$5,000 they'd do it on the spot. So all law enforcement can do is sit around and wait for the telephone company to come in with the evidence, which hardly ever happens."

—Do you have any qualms about the work you're doing?

"If I had a conscience in this business I couldn't stay in it. Moral feeling doesn't exist here as far as I'm concerned. I look at

two things: money and risk. Don't forget, I've been as low as you can get, penniless, on drugs. The bugging scare today has reached the point of paranoia, so much so that your average citizen thinks people like me are slime. Well, it's not a bad business. I manufacture a product. Like a gun it can be used for good or bad. If my equipment keeps some drugs out of the country, that's fine. I take a dim view of pushers. If the liberal objects to bugging, I tell him to wait until his daughter gets hooked on drugs and then he won't be so particular about protecting the pusher's rights."

—Do you do any personal bugging?

"No, I know what my wife's up to. In the beginning I bugged for laughs. I overheard my mother-in-law cursing me, but she's dead now. Oh, yes, I wired my own phone once to make a tape of a guy who was working with Peter and me. He wanted me to help him cut Peter out of a deal. I taped everything he said and gave it to Peter, and Peter threw him out of the business."

—What would you do if you found a wire on your own phone?

"I'd be cool. I'd just take it off and put it on someone else's phone."

EXHIBIT NO. 1

ELECTRONIC SURVEILLANCE EQUIPMENT SALES ANALYSIS

To determine the scope and nature of business being conducted by manufacturers* of electronic surveillance equipment, and the degree of compliance with 18 USC 2512, the Commission staff asked a number of manufacturers to make their sales records available for analysis. The records of the following firms were examined:

Audio Intelligence Devices
Bell & Howell Communications Company
R. B. Clifton Company
B. R. Fox Company, Inc.
Fargo Company
Martin L. Kaiser, Inc.
Laser Enterprises
Security Specialists, Inc.
Tracer Investigative Products, Inc.

The information obtained from the records indicates an attempt on the part of the manufacturers to adhere to the provisions of Section 2512, although a lack of uniformity in the record keeping systems and sales procedures of the various companies makes it difficult to reach any broad conclusions. For one thing, there was great variation in the period of time covered by the records of the different companies. More importantly, there were variations in the procedures covering such areas as determining the identity of the purchaser, recording the details of the transaction, and establishing criteria for what constitutes a device "primarily useful for the purpose of surreptitious interception of wire or oral communications."

The last term is of particular importance because it determines to whom the manufacturers will or will not sell a particular device. Some manufacturers deal only with government agencies, and certain of those will sell only to government agencies that constitute a U.S. intelligence service or have the power of arrest; others sell to private individuals and firms as well as government agencies. Those who sell to private sources must draw a line between non-prohibited devices and those which constitute "primarily useful" devices.

*For the purpose of this report the terms manufacturer and distributor will be used interchangeably.

Unfortunately the line between prohibited and non-prohibited devices is not easy to draw. A basic difficulty arises from the fact that any device which is designed to overhear conversations can also be used for one-party consent monitoring. For example, the legislative history of Title III (the Federal Wiretap Act), as outlined in Senate Report No. 1097, April 29, 1968, (p. 95), gives as examples of "primarily useful" devices the microphone disguised as a wristwatch, cufflink, fountainpen, or tie clip. Yet it would be hard to imagine these devices being used for anything but one-party consent monitoring.

The advent of integrated circuitry has provided the technology for building smaller and more efficient transmitters. Although these transmitters, sometimes described as microminiature or subminiature, have the potential for use in interception of wire or oral communications, they are not necessarily prohibited under Section 2512. In fact, the legislative history referred to above states: "A device does not fall under the prohibitions merely because it is small, or because it may be adapted to wiretapping or eavesdropping."

Thus we have a proliferation of modern devices which pose a far greater danger to privacy than the majority of the devices mentioned in the legislative history of Title III. This danger might be lessened by broadening the definition of prohibited devices. This solution, however, could create havoc among those engaged in the production of electronic equipment for legitimate purposes (i.e., the communications and entertainment industries).

One area of the statute which causes difficulty for the manufacturers of electronic surveillance equipment is Section 2512(2)(b), which provides an exception for "an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, *in the normal course of the activities of the United States, a State or a political subdivision thereof* . . . " The manufacturers have decided that it is not their responsibility to determine if a law enforcement officer or agency is authorized to use the equipment and indeed will use it "in the normal course of activities." One question that

is not easy to answer is whether a police officer or department can purchase or possess prohibited devices in a state that does not have legislation authorizing court-authorized wiretaps.

The Commission asked the Department of Justice for its interpretation of "in the normal course of activities." A portion of the response offered by John C. Keeney, Acting Assistant Attorney General, follows (for a more detailed answer to this and other questions, see Tab —, Exhibit No. —):

If a state has no authorizing statute for the purpose of meeting the requirement of 18 USC 2516(2), it cannot be in the normal course of activities of state and local police departments in that state to intercept communications without at least one party consent. Accordingly, it cannot be in the normal course of their activities to possess equipment primarily useful for the nonconsensual interception of communications. However, one party consensual interceptions are permissible under the federal electronic surveillance statute if intercepted "under color of law," 18 USC 2511(2)(c). So long as such intercepts are permitted under state law, the state and local police may legally engage in one party consent intercepts. Since such intercepts would then be both legal and for a law enforcement purpose, the equipment used is exempted from the prohibitions of Section 2512(1).

Accordingly, even though the state is a "non-authorization state" it would be legal for police departments to possess those devices proscribed by Section 2512(1) which are designed for one party consent interceptions. It would not, however, be legal for them to possess devices designed for nonconsensual interceptions.

The following sales record analysis will give the Commission members an opportunity to note the difficulties involved in determining which devices should be considered "primarily useful," and the equally complex problems involved in trying to categorize devices according to their functions in order to conform to selective state statutes.

It should be noted that the following analysis represents only a small portion of the total sales output of each manufacturer; for the purposes of these hearings we have included only those devices which are prohibited or which fall into the large grey area of being probably or possibly prohibited. The purchasers of the devices are listed by state only and not by individual department.

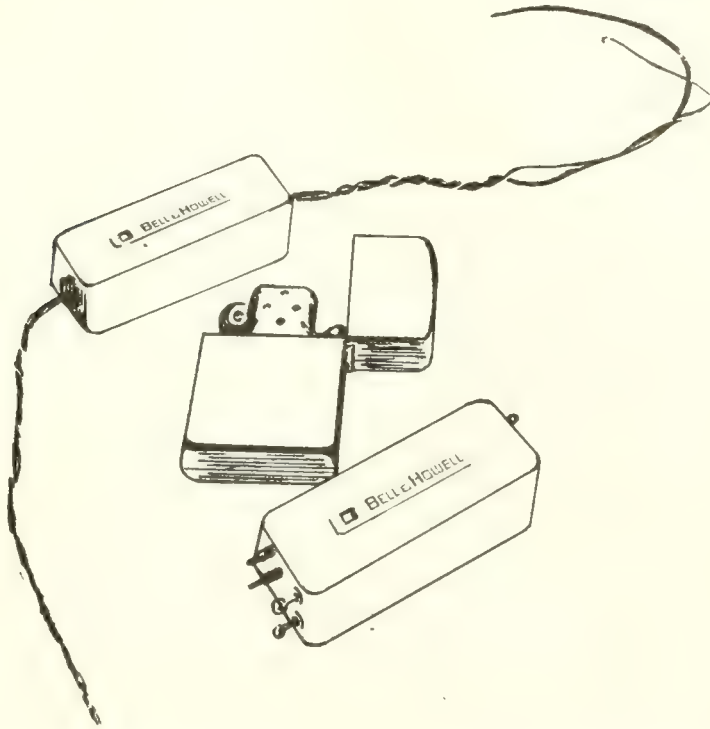
BELL & HOWELL COMMUNICATIONS COMPANY
EQUIPMENT SALES
1973 and 1974

*EQUIPMENT	PURCHASER Private Enterprise	** U.S. Government	States With Authorization Statutes	States Without Authorization Statutes (by state and quantity)
T8	0	0	8	0
T8C	0	4	0	Ca.-2 (2)
T-12MFM	0	1	14	0
T-11	0	0	4	La.-6 Oh.-2 Wy.-1 (9)
T-57	0	0	1	Al.-1 Ca.-1 Wy.-1 (3)
R-57B	0	0	1	Il.-1 La.-5 Oh.-1 Ms.-2 (9)
SK-6	0	9	1	Ca.-1 La.-1 (2)
AGC-3	0	12	10	Al.-1 Pa.-2 Ca.-2 Il.-1 Mi.-3 Mo.-1 Oh.-4 (14)

* For detailed description of equipment see attached advertisements

**Includes sales to DEA, IRS, and Customs.

200 MILLIWATT REMOTE POWERED MINATURE FM TRANSMITTER
30-50 MHz 150-174 MHz



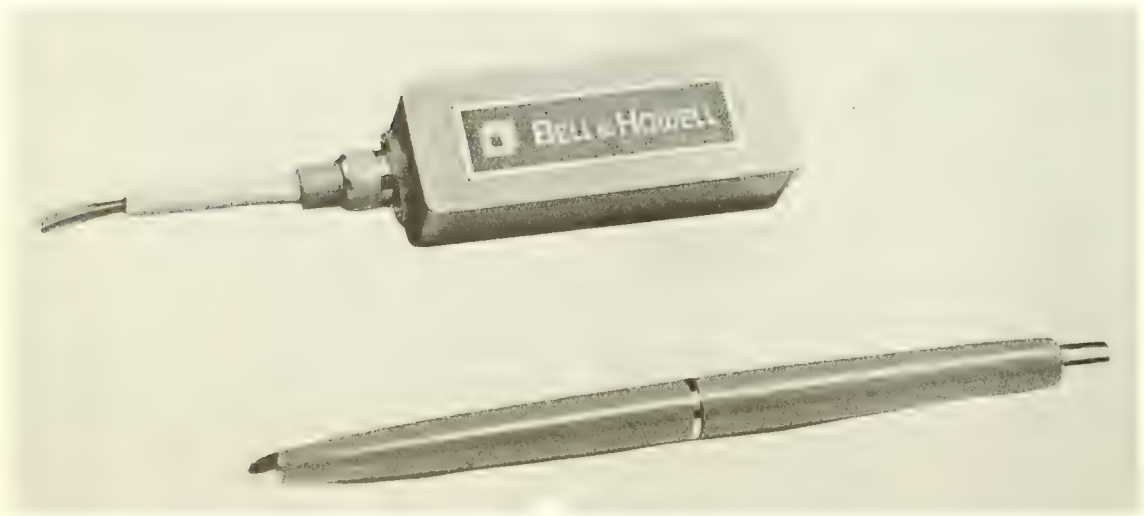
The T-8 Transmitters are high reliability transmitters with water seal integrity options available.

The unit is of modular construction of the same designs as our superior T-2 Transmitter, with the same basic specifications applicable.

Model T-8 is a completely sealed unit using minature glass seal terminals for input and output connections.

T-8/C Miniature FM
Transmitter

200 MILLIWATT REMOTE POWERED MINIATURE FM TRANSMITTER
30 - 50 MHz 150 - 174 MHz



This fine transmitter is another addition to the line of low powered miniature transmitters.

The unusual feature of this instrument is a unique RF connector incorporating all inputs and outputs.

The connector is a go - no go, configuration with twist locking and is designed to assure easy field installations.

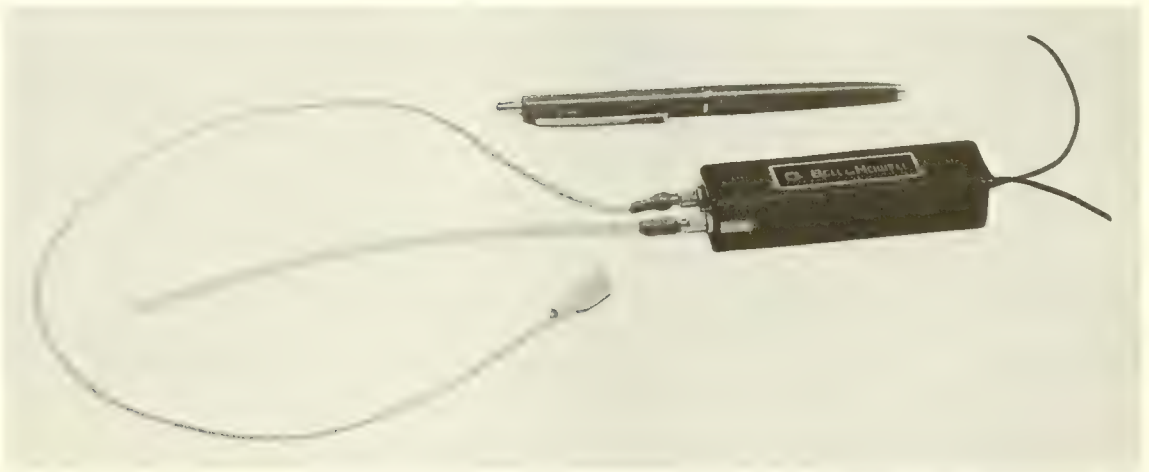
RESTRICTED EQUIPMENT

1 WATT MINIATURE VHF TRANSMITTER

30-50 MHz

148-174 MHz

(FCC Type Accepted)



This device is the remote powered version of the Model T-12 Transmitter.

Audio circuits are the same compression type made famous in the Model T-2, T-12 and 247 Transmitter.

The Audio input and RF output are through miniature, but rugged, (27 series) amphenol connectors with the power supply connected to the flying leads.

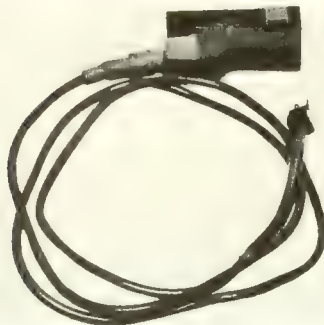
The unit is supplied less microphone and antenna, but with matching male connectors.

RESTRICTED EQUIPMENT

T-11

Telephone Line Transmitter—Miniature, crystal controlled telephone line transmitter. This transmitter works in series with and derives its operating power from the telephone line on which it is installed. It has the capability of transmitting both sides of a telephone conversation to a remote receiver. (Photograph not available.)

T-57 CLAMP-ON PICKUP



This unit serves in lieu of the microphone
when installed over telephone cables.

R-57B

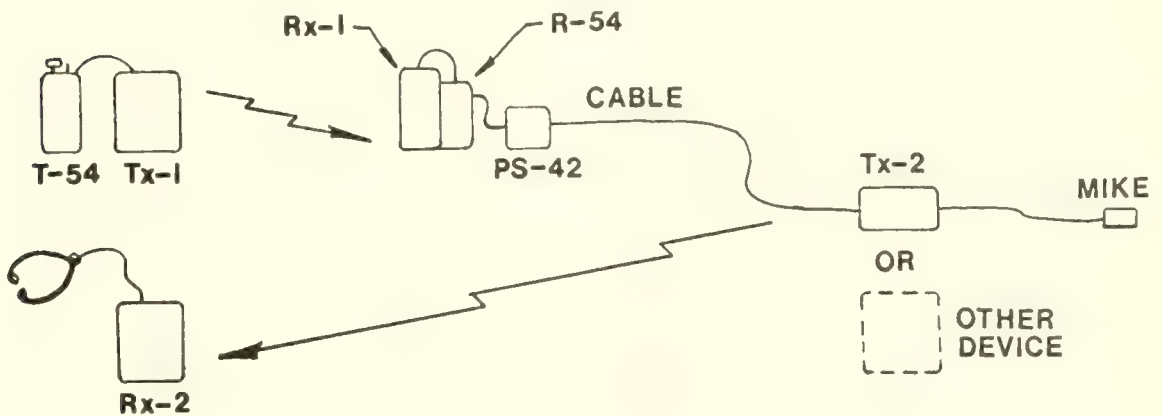
Remote Relay & Monitoring Adapter—This device allows distant monitoring by telephone of information emanating from a transmitter. The transmitter is placed in an area to intercept conversations, and a receiver is located within receiving range.

The receiver is plugged into the R-57B adapter which is connected across telephone lines. All conversations are relayed to the point of connection of the adapter. The conversations can then be monitored by dialing the number of the telephone line at which the adapter connection is made. (Photograph not available.)

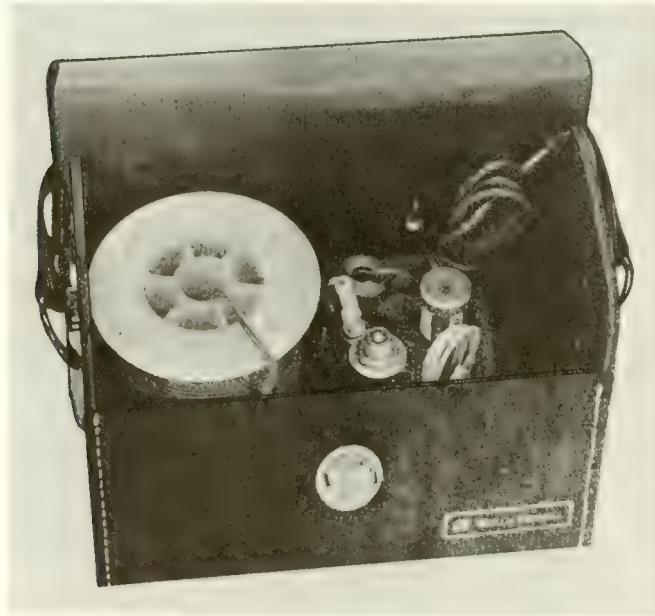
REMOTE TONE ACTIVATION OF TRANSMITTER - POWER SUPPLIES
VHF - FM HI OR LO BANDS
OR
UHF - 406 to 420 and 450 - 470 MHz Ranges



This sophisticated package allows operation (on or off) of transmitters or other devices from remote locations - a needed capability when the intelligence operation is faced with countermeasure activity or programmed 'off' conditions are an operational necessity.



K-AGC-2 AMPLIFIER BOOSTER KIT



The AGC-2 amplifier booster kit has been provided as a result of experience with the difficulties encountered in attempting to covertly transmit from the shielded areas of a building with low power radio. The booster allows the microphone and amplifier to be in the intercept area while transferring the information thru a cable to a most favorable located transmitter.

The AGC amplifier is a highly sensitive circuit sealed into a strong, magnetically shielded case. The amplifier offers the advantage of volume contraction, or automatic gain control. Loud signals, (voices near the microphone) are instantaneously and automatically less amplified than are quieter signals (Softer voices at a distance from the microphone).

The action of the AGC-2 is automatic and instantaneous, no controls are provided and adjustments are not required. In addition to automatic control the AGC-2 amplifies the signal to such a level that it can effectively tranverse a long cable to the transmitter. This allows ordinary two-conductor line, flat line, twisted pair or shielded cable to be used, as the interconnect.

AUDIO INTELLIGENCE DEVICES EQUIPMENT SALES 1972

*EQUIPMENT PURCHASER

	Private Enter- prise	**U.S. Gov- ern- ment	States With Authori- zation Statutes	States Without Authorization Statutes (by state and quantity)
U-140.....	0	0	0	0
TA-400.....	0	0	2	0
TX-651.....	0	0	1	0
TX-651A...	0	0	0	0
TX-702.....	0	0	0	0
TX-755.....	0	0	0	0
TX-801.....	0	0	2	La.-1 W. Va.-2 (3)
TX-805.....	0	0	4	La.-1 Tex.-4 (5)
AP-1100...	0	0	0	0

* For detailed description of equipment see attached advertisements

** AID did not report sales to U.S. agencies

AUDIO INTELLIGENCE DEVICES EQUIPMENT SALES 1973

*EQUIPMENT PURCHASER

	Private Enter- prise	**U.S. Gov- ern- ment	States With Authori- zation Statutes	States Without Authorization Statutes (by state and quantity)
U-140.....	0	0	3	Ill.-1 Utah-1 (2)
TA-400.....	0	0	3	Utah-1 (1)
TX-651.....	0	0	2	0
TX-651A...	0	0	0	0
TX-702.....	0	0	3	Ky.-1 N.C.-2 (3)
TX-755.....	0	0	2	0
TX-801.....	0	0	3	Utah-3 (3)
TX-805.....	0	0	8	La.-1 Mich.-2 Miss.-1 Utah-2 (6)
AP-1100...	0	0	0	0

AUDIO INTELLIGENCE DEVICES EQUIPMENT SALES 1974

*EQUIPMENT PURCHASER

	Private Enter- prise	**U.S. Gov- ern- ment	States With Authori- zation Statutes	States Without Authorization Statutes (by state and quantity)
U-140.....	0	0	5	Ind.-2 La.-1 N.C.-1 S.C.-2 (6)
TA-400.....	0	0	5	La.-2 (2)
TX-651.....	0	0	1	Ind.-1 Mich.-1 (2)
TX-651A...	0	0	4	0
TX-702.....	0	0	13	Ala.-2 Idaho-1 Ill.-1 Utah-1 Ky.-1 La.-6 Mo.-1 Tenn.-1 Tex.-1 N.C.-1 W. Va.-1 (17)
TX-755.....	0	0	14	Ala.-4 Cal.-2 Ky.-1 N.C.-1 La.-2 Mich.-3 Tex.-1 Utah-1 W. Va.-1 (16)
TX-801.....	0	0	4	Ky.-3 La.-1 W. Va.-2 (6)
TX-805.....	0	0	13	Ala.-5 Ky.-3 La.-5 Mo.-1 Mich.-1 Miss.-1 N.C.-1 Tex.-1 Tenn.-1 W. Va.-1 (20)
AP-1100...	0	0	2	Cal.-1 La.-2 Mich.-3 (6)

AUDIO INTELLIGENCE DEVICES EQUIPMENT SALES 1975 (to May 1)

*EQUIPMENT PURCHASER

	Private Enter- prise	**U.S. Gov- ern- ment	States With Authori- zation Statutes	States Without Authorization Statutes (by state and quantity)
U-140.....	0	0	0	Ill.-1 (1)
TA-400.....	0	0	0	0
TX-651.....	0	0	1	0
TX-651A...	0	0	0	Miss.-2 (2)
TX-702.....	0	0	6	Cal.-1 Ind.-1 N.C.-1 Tex.-1 (4)
TX-755.....	0	0	5	Ind.-1 Miss.-2 Mont.-2 Tex.-1 (6)
TX-801.....	0	0	2	Mont.-1 (1)
TX-805.....	0	0	4	Miss.-2 Mont.-1 (3)
AP-1100...	0	0	0	0

UNITEL[®] 140

INTELLIGENCE RECORDING SYSTEM



The UNITEL[®] 140 is a completely self-contained recording system, housed in a standard three inch attache' case, modified to include a hidden built-in microphone and remote actuation switch.

A high quality cassette tape recorder, with AGC circuitry, utilizes an amplified microphone built into the case, and may be remotely controlled by a small concealed switch beneath the handle of the attache' case. Four "C" cell batteries will power the unit for up to seven hours.

Adaptor cables and accessories fit into special compartments cut into the polyethylene foam lining of the UNITEL[®] 140, and the recorder itself may be easily removed for use outside the case with standard microphone components.

Another model, using the MR-15 recorder in a five inch attache' case, is available as the UNITEL[®] 141.

SPECIFICATIONS

POWER REQUIREMENTS: Recorder: 117 VAC, 60 Hz; 6 VDC, 4 each Mallory MN-1400 Alkaline "C" cells or equivalent. Automobile battery adapter cable (optional). **Microphone:** 1.5 VDC, 1 each Mallory MN-1400 Alkaline "C" cell or equivalent.

POWER CONSUMPTION: AC: 3W.

TAPE CASSETTE: Sony C-30 (30 min.), C-60 (60min.), C-90 (90 min.), or C-120 (120 min.) or equivalent tape cassette.

TAPE SPEED: 1 7/8 ips.

TRACKS: 2-track monaural.

SPEAKER: 4 x 2 3/4", dynamic.

POWER OUTPUT: 1.5 W.

FREQUENCY RESPONSE: 50 - 10,000 Hz.

INPUTS: Microphone Input Jack, sensitivity -72 db (0.2 mV), Low impedance; Auxiliary Input Jack, sensitivity -22 db (0.06 V), input impedance 100 k; Remote Control Jack.

OUTPUT: Monitor Jack, output level 0 db (0.775 V), suitable load impedance 10 K or an 8-ohm earphone.

BATTERY LIFE: 7 hours continuous (approximate) with 4 Mallory MN-1400 Alkaline "C" cells.

SUPPLIED ACCESSORIES: C-60 Tape Cassette; 4 each MN-1400 "C" cells; Earphone; AC Power Cord; Short Plug; Microphone F-26S; Remote Control Cable; Connecting Cable RK-6g.

OPTIONAL ACCESSORIES: Automobile Battery Adapter Cable; Head Demagnetizer; Cassette Eraser; Microphone Extension Cable.



CASE: 18 1/2 in. (470 mm.) x 13 1/2 in. (343 mm.) x 3 in. (76 mm.).

WEIGHT: 11 1/2 lbs. (5.2 kg.) including recorder, batteries and accessories.

AUTOMATIC TELEPHONE RECORDING ACTUATOR

TA-400

NO RELAYS

FULLY PORTABLE

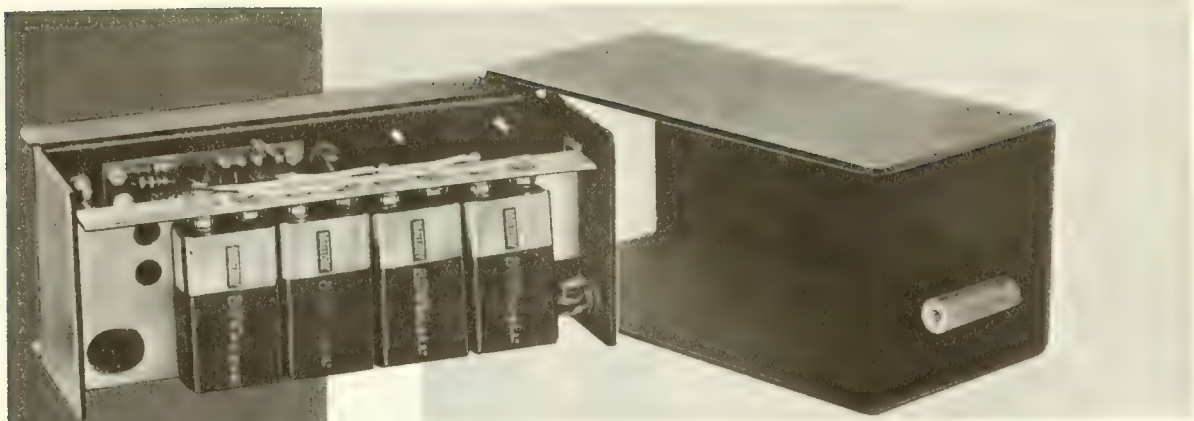
BATTERY POWERED



The TA-400 is designed for use with the MR-16 portable intelligence recorder, but will work equally well with most other high quality DC operated recorders. It is especially useful where space and installation time are critical and where AC power is not available.

As the telephone handset is picked up, the unit automatically switches the recorder on and records every sound, including dial tones and pulses, until the handset is replaced and the recorder stops. Solid state switching provides reliable noise-free operation, eliminating the need for troublesome relays, on either regular or pay phones. Powered by four standard 9-volt alkaline transistor radio batteries, the TA-400 will operate up to two months under normal phone use and cannot be readily detected because it is electrically isolated from the line itself.

Binding posts secure telephone line connections and a dial tone test pushbutton serves to check tape recorder functions after connection to the TA-400. Battery condition is displayed on a front panel meter.



SPECIFICATIONS

POWER SOURCE: Four 9V batteries, Mallory MN-1604 or equivalent.

BATTERY LIFE: Up to 2 months operation at normal (20°C) 68°F ambient temperature.

CIRCUITRY: All solid-state.

TELEPHONE INPUT: Direct line connection, polarity immaterial.

LINE ISOLATION: Complete electrical isolation from the telephone line.

OUTPUTS: Audio output to tape recorder. Recorder Control; solid-state switch with 1 Amp capacity.

CONTROL CABLES: 2 each furnished with unit.

CONTROLS: On-Off, Dial Tone, Battery Test.

CONNECTIONS: Binding posts for telephone input. Micro jack audio output. Miniature jack recorder control.

METER: Self-contained 0-15 VDC for momentary check of battery voltage.

CASE: Aluminum.

SIZE: 4 1/2" x 2 3/4" x 2"

WEIGHT: 1 lb.

REGULAR/PAY PHONE OPERATION: Automatic transfer of mode of operation with adjustable threshold points.

Copyright © 1973 by Audio Intelligence Devices, Inc. No part of this publication may be reproduced in part or full without the written consent of Audio Intelligence Devices, Inc.

Telephone Actuated Transmitter

Model TX 651 141-175 MHz



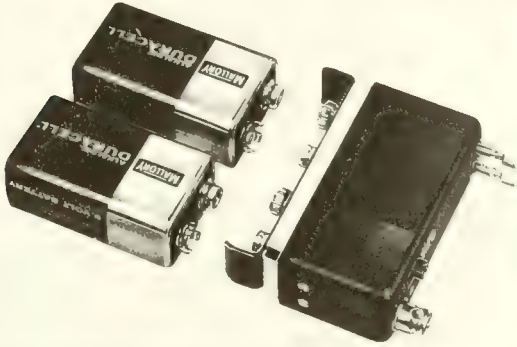
The TX 651 crystal-controlled telephone transmitter is compatible with virtually all telephone systems and has been designed to operate only when the telephone line is actually in use. The transmitter is automatically activated by the drop in voltage when the telephone handset is lifted, and upon completion of the call, the transmitter instantly switches itself off.

Powered by its own self-contained batteries, the TX 651 is not readily detectable and will operate for over a month on two standard 9V alkaline cells, transmitting both sides of the conversation with a power output of 50 milliwatts. An optional mercury battery pack will increase the output power to 100 milliwatts while extending battery life to over three months.

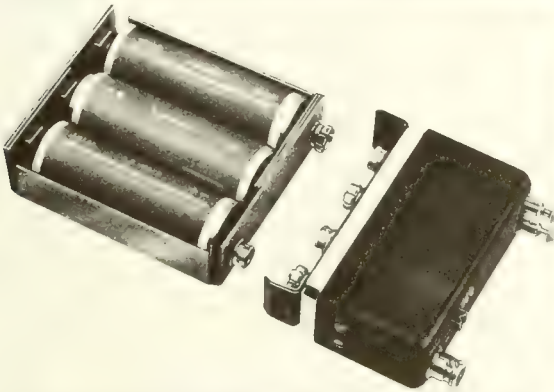
The small size of the TX 651 provides unlimited concealment possibilities anywhere on the telephone signal pair between the instrument and telephone central office. The TX 651 uses no microphone since it is modulated directly by the telephone line. These transmitters are ideal for use with all AID Intelligence Systems equipped with VHF FM receivers operating on the same frequency.

Proprietary Information - Not an offer to sell

SPECIFICATIONS



TX 651 shown with 2 standard 9 Volt Alkaline batteries.



...with the optional 3 cell mercury pack for extended life.

RF POWER OUTPUT: 50 mW into 50 Ohm load @ 9V DC.

FREQUENCY RANGE: 140-175 MHz.

CRYSTAL: Crystal frequency to customer's specifications.

FREQUENCY STABILITY: ± 10 ppm from -4°F (-20°C) to 68°F ($+20^{\circ}\text{C}$) ambient temperature.

HARMONICS: 43 db below rated output power.

MODULATION: ± 5 KHz deviation maximum with standard line signal.

AUDIO RESPONSE: 300 to 3000 Hz with 6 db per octave pre-emphasis.

ACTUATION: "OFF" with 18 to 50V across telephone pair. "ON" with less than 18V across telephone pair.

ACTUATOR DRAIN: 200 microamps.

ANTENNA: Flexible wire.

CONTROLS: On-Off switch.

CONNECTIONS: MB antenna connector, binding posts for telephone line connection.

BATTERY REQUIREMENTS: Standard, 2 each Mallory MN 1604 9V alkaline-manganese cells or equivalent. For extended life, 3 each Mallory TR 133 4.2V mercuric-oxide cells with special holder is available at additional cost.

BATTERY LIFE: Over one month with standard batteries under normal telephone use. Up to three months using 3 mercuric-oxide cells, under similar operating conditions.

CASE: Stainless steel, black matte epoxy finish.

SIZE: 2 7/8 in. (73 mm.) x 2 1/4 in. (57.1 mm.) x 3/4 in. (19 mm.) with standard batteries, excluding hardware.

WEIGHT: 13 1/2 oz. (382.7 g.) including standard batteries.

Our program of continual reevaluation for possible improvement makes these specifications subject to change without notice.

MODEL TX702

MICRO-MINIATURE TRANSMITTER

COMPLETELY SELF-CONTAINED

AID's TX 702 micro-miniature transmitter is a completely self-contained unit, including antenna, ultra-sensitive microphone, and batteries. Small on size, big on performance, the TX 702 is easily concealed and provides maximum effectiveness with fast installation and a minimum risk of detection.

HEARING AID TYPE BATTERIES

There are no controls of any kind to be tampered with on the TX 702. Inserting a common hearing aid type battery activates the transmitter and powers it continuously for over eleven days. Higher power output may be obtained, with some reduction in battery life, by inserting two or three batteries as required.

Compatible with any professional quality wide band FM receiver tunable over the 37.5 to 39.5 MHz range, these transmitters are particularly well suited for use with the AID 870 and 875 crystal/tunable FM intelligence receivers.

These are the first sub-miniature transmitters of a quality practical for rigorous field requirements. Designed, built and tested in AID's own laboratories, the TX 702 transmitters are quality controlled to exacting standards for use under difficult environmental conditions.



Proprietary Information - Not an offer to sell

SPECIFICATIONS



RF POWER OUTPUT INTO 50 OHM LOAD:
With one battery: 0.5 mW; With two batteries: 1.5 mW; With three batteries: 2.5 mW.

FREQUENCY RANGE: 37.5 to 39.5 MHz.

FREQUENCY STABILITY: 10 KHz/hour after warmup.

MODULATION: Wide band FM.

SENSITIVITY: 75 db below 1 volt RMS/Microbar pressure for 15 KHz deviation.

ANTENNA: Flexible wire, integral, 60 in. (152 cm.).

MICROPHONE: Self-contained.

BATTERY: One, two or three Mallory MS-76 silver oxide or equivalent.

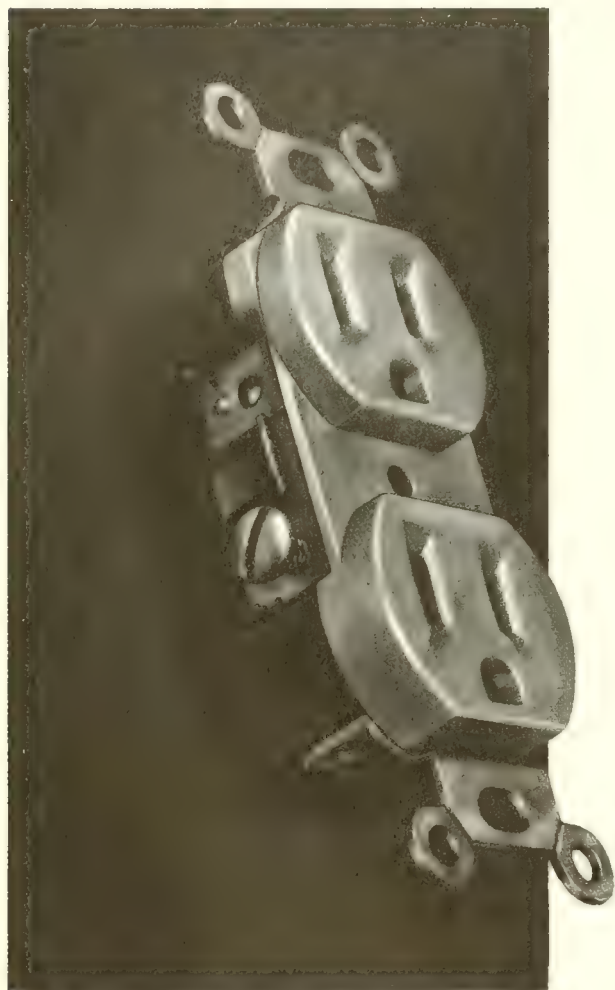
BATTERY LIFE: One battery: 270 hours; Two batteries: 150 hours; Three batteries: 60 hours. Above figures for continuous operation at 68°F (20°C) ambient temperature.

SIZE: Height: 1 9/16 in. (40 mm.); Diameter: 9/16 in. (14 mm.).

WEIGHT: 3/4 oz. (21 g.), including three batteries.

Our program of continual reevaluation for possible improvement makes these specifications subject to change without notice.

LIFE	MS-76	POWER
270 hrs.		0.5 mW
150 hrs.		1.5 mW
60 hrs		2.5 mW



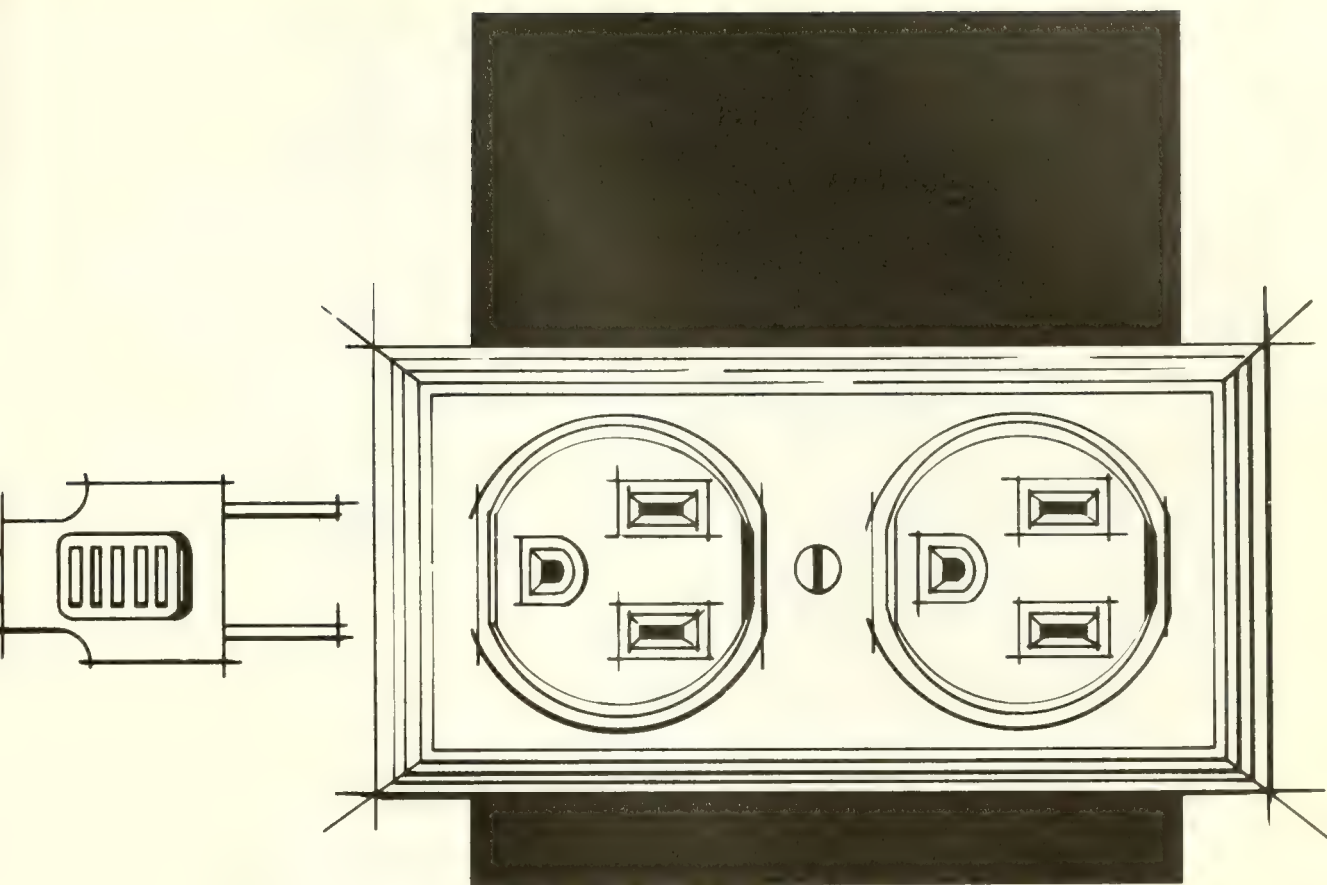
TX 755

TRANSMITTER

**REPLACES ANY
STANDARD
OUTLET**

The TX 755 looks and functions just like the ordinary duplex wall outlet it replaces. You can even plug in an electrical appliance while the skillfully concealed amplified microphone and AC powered transmitter molded into it allow you to monitor every sound without interruption.

Because it draws power directly from the AC line there are no batteries to charge and, because it radiates a signal from that same AC line, there is no separate antenna to string. The standard wall outlet is simply removed with the aid of a screwdriver and the TX 755 installed in its place.



SPECIFICATIONS

OPERATING FREQUENCY: 35 to 39 MHz (If not specified by purchaser, actual frequency will be selected by AID. If a precise frequency is requested, allow 30 days ARO).

FREQUENCY STABILITY: Less than $\pm 1.0\%$ deviation after 15 minutes operation.

FREQUENCY CONTROL: Temperature Compensated High "Q" circuit.

NOMINAL POWER OUTPUT: 25 mW minimum into a 50 Ohm load.

OPERATING VOLTAGE: 115 VAC - 60 Hz nominal, 150 VAC - 60 Hz maximum.

CURRENT DRAIN: 15 mA maximum @ 117 VAC

MICROPHONE AMPLIFIER: Deviation Control with High Gain Compression.

FREQUENCY DEVIATION: ± 25 KHz nominal.

POWER SUPPLY: Self-contained constant current.

HUM: 40 db minimum below a 1 KHz standard deviation signal.

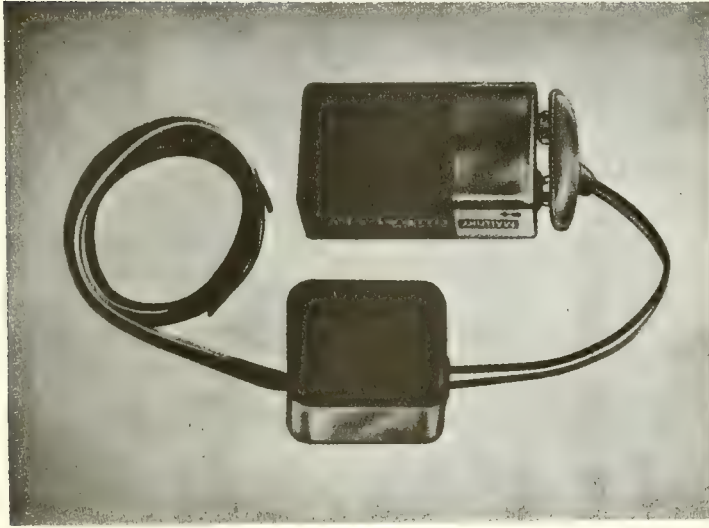
ANTENNA: AC Power Line Coupled.

OUTLET: Standard duplex 3 conductor grounded type, ivory or brown.

COVER PLATE: To match outlet, mounting screws included.

RECOMMENDED RECEIVER: AID RX 870 or RX 875 with automatic frequency control

MINIATURE TELEPHONE TAP TRANSMITTER—MODEL 801



**PRESET
36 to 50 MHz
FREQUENCY**

Over 3 Days Continuous Operation

**SUB-MINIATURE
WIDE BAND FM**

The AID Model 801 Miniature Telephone Tap Transmitter is an inconspicuous unit designed to take on the appearance of standard telephone equipment. It is small enough to be completely concealed inside most conventional desk telephones or it may be installed at any point on the telephone line between the instrument and the central office.

A carefully controlled output signal of 25 mw permits monitoring at a safe distance, yet minimizes the possibility of chance interception. This unit is ideal for use with the AID 870 Receiver and R-15 Recorder.

**WEATHERPROOF
EASILY CONCEALED**

Powered by a single 9V alkaline battery, the 801 Miniature Telephone Tap Transmitter will transmit continually for three days at normal room temperatures. A line coupler is provided for utilization of the telephone line as an antenna, or a 36" length of wire may be attached for added distance. All wires are connected to external pins located on the bottom of the unit so that they may be detached or replaced easily.

Designed and torture-tested in AID's own laboratories, this device incorporates the very latest state-of-the-art concepts and is without equal in the industry.



SPECIFICATIONS

SIZE:	1 1/8 x 7/8 x 3/4 (not including battery).	MODULATION:	± 50 KHz deviation on standard telephone lines.
RF POWER SUPPLY:	25 mw into a 50 ohm load.	AUDIO FREQUENCY RESPONSE:	300 to 4000 Hz governed by telephone line transmission.
BATTERIES:	See chart below	ANTENNA:	Telephone line or 36" length of wire for added distance.
FREQUENCY RANGE:	36 to 50 MHz (as per customer requirements).	MICROPHONE:	None — modulation from telephone only.
FREQUENCY CONTROL:	Free-running	CASE:	Marine aluminum alloy with matte black finish.
FREQUENCY DRIFT:	Less than 10 KHz drift per hour under normal environmental conditions depending upon battery used.	COMMENTS:	Weatherproof.

BATTERY LIFE — CONTINUOUS DUTY

Battery Life Shown is Based on 70°F Operating Temperature

BATTERY	VOLTS	NO. REQ.	TYPE	TEMP. RANGE	MODEL 801
TR-146X	9V	1	Mercury	45° — 110°F	80 hrs.
MN-1604	9V	1	Alkaline	10° — 110°F	72 hrs.
216	9V	1	Carbon-Zinc	20° — 80°F	9 hrs.

**FAST AND EASY INSTALLATION • UN-
LIFE • LOW POWER • NO BATTERIES**

TELEPHONE DROP-IN TRANSMITTER



MODEL TX-805
37.5 TO 38.5 MHz

Replaces telephone mouthpiece cartridge.

Transmits both sides of conversation.

Turns "ON" when handset is lifted.

Turns "OFF" when handset is placed in cradle.

- ▶ **NO ANTENNA**
- ▶ **NO WIRING**
- ▶ **NO EFFECT ON TELEPHONE**
- ▶ **NOT EASILY DETECTED**
- ▶ **QUALITY UNSURPASSED**



SPECIFICATIONS

SIZE: 1.5 inch diameter, 0.25 inch high.

RF POWER OUTPUT: 2.0 mW into a 50 ohm load at 6V line voltage.

FREQUENCY RANGE: 37.5 to 38.5 MHz.

FREQUENCY STABILITY: 20 KHz/hour after warmup and at constant temperature.

MODULATION: Frequency modulation, 50 KHz deviation at normal line levels.

ANTENNA: Automatically connected to line.

BATTERY: Not required.

MICROPHONE: Self-contained.

RECOMMENDED RECEIVER: AID Model RX-870 in AFC Mode.

Our program of continual reevaluation for possible improvement makes these specifications subject to change without notice.

AP-1100

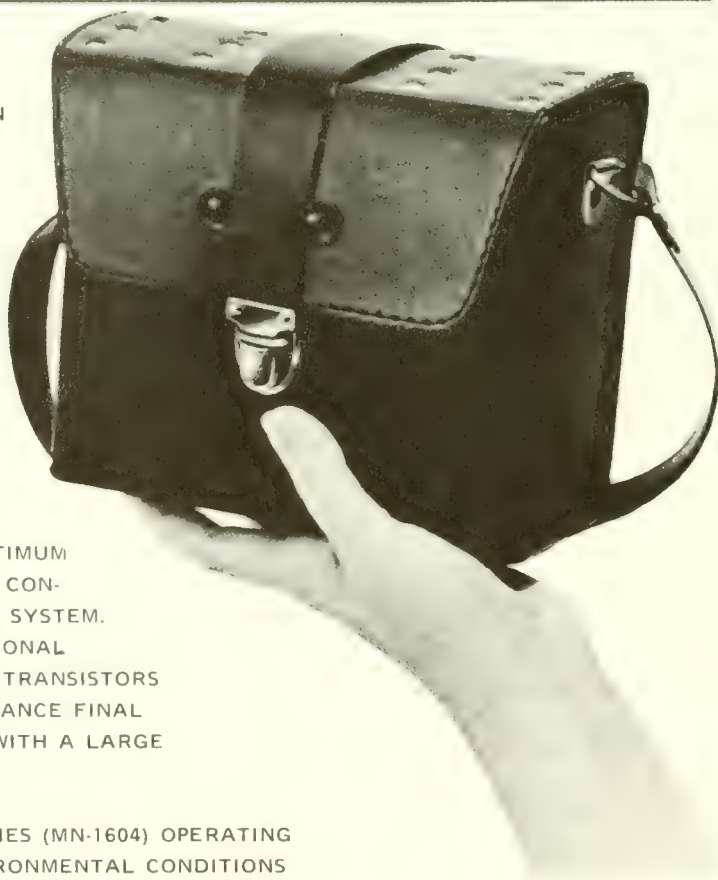
MICROPHONE AMPLIFIER KIT

THE AP-1100, A WIREBOUND TRANSMISSION SYSTEM, HAS BEEN DESIGNED FOR AND IS INTENDED FOR USE IN SOUND INTERCEPTION APPLICATIONS REQUIRING TRANSMISSION OVER SHORT TO EXTREMELY LONG CABLE RUNS. CONTROLLED AND LIMITED BY THE BANDPASS CHARACTERISTICS OF THE AMPLIFIER, THE FREQUENCY RANGE OF SOUND TRANSMISSION IS FROM 200 TO 6000HZ, THUS ASSURING EXCELLENT QUALITY RECORDING AND SUBSEQUENT REPRODUCTION.

THE AID AMPLIFIER IS DESIGNED FOR OPTIMUM PERFORMANCE USING THE HIGH QUALITY CONDENSER MICROPHONE SUPPLIED WITH THE SYSTEM. THE AMPLIFIER EMPLOYS FOUR OPERATIONAL AMPLIFIERS AND JUNCTION FIELD EFFECT TRANSISTORS FOR GAIN CONTROL. A VERY LOW IMPEDANCE FINAL AMPLIFIER PERMITS PROPER OPERATION WITH A LARGE VARIETY OF LOAD IMPEDANCES.

POWERED BY TWO 9 V ALKALINE BATTERIES (MN-1604) OPERATING LIFE OF 60 HOURS UNDER NORMAL ENVIRONMENTAL CONDITIONS IS PROVIDED.

A CABLE RUN OF 6 MILES OF 150 OHMS, 10 MILES OF 600 OHM CABLE, TELEPHONE LINE, OR ORDINARY TV TWIN LEAD MAY BE USED AS TRANSMISSION LINES.



COMPONENTS



CARRYING CASE
MICROPHONE AMPLIFIER
CONDENSER MICROPHONE WITH CABLE
TERMINATION UNIT TU-1
TERMINATION UNIT TU-2
CABLE AND REEL (100 FEET)
TWO C-5 CABLE ASSEMBLIES
EARPHONE CABLE ASSEMBLY
RIGHT AND LEFT EARPLUGS
TWO MN-1604 ALKALINE
DURACELL® BATTERIES

SPECIFICATIONS

AMPLIFIER

GENERAL

SIZE: 2 1/4" x 3 1/4" x 3/4" (5.7 x 8.2 x 2 cm.).

WEIGHT: 6 1/2 oz. (185 gr.).

BATTERY: 9V Alkaline, MN-1604, 2 each.

OPERATING LIFE: 60 hrs. continuous @ 68°F
(20°C) ambient temperature.

CONTROLS: ON-OFF combined with VOLUME.

CONNECTORS: Microphone - 0.1" Dia. Subminiature
Phone (output) - 0.140" Dia. Miniature.

ELECTRICAL

INPUT IMPEDANCE: Optimized for Condenser
Microphone approximately 2000 ohms.

GAIN: 50 db minimum closed loop.

OUTPUT: 2mW minimum into 1000 ohm load.

DYNAMIC RANGE: 50 db minimum.

AGC: No more than 3 db change in output for 50 db
change in input level.

FREQUENCY RANGE: 200 Hz to 6000 Hz @ -3 db
points.

COMPLEMENT: 4 each Integrated Operational
Amplifiers; 2 each Junction Field-Effect Transistors;
2 each Diodes.

LOAD IMPEDANCE: 100 ohms to 50,000 ohms.

TERMINATION UNITS

TU-1

LOAD IMPEDANCES: 150 ohm unbalanced (coaxial
or shielded cable). 600 ohm balanced (twisted pair,
TV lead).

PRIMARY: 1000 ohm unbalanced.

FREQUENCY RANGE: 200 Hz to 10,000 Hz @
3 db limits.

POWER LEVEL: 25 mW maximum.

CONNECTORS: Input - Screw Terminals. Output -
0.14" Dia. miniature.

SIZE: 1 1/4" Dia. x 3 1/4".

WEIGHT: 3 oz. (85 gr.).

TU-2

INPUT IMPEDANCES: 150 ohm unbalanced. 600
ohm unbalanced.

OUTPUT: 1,000 to 50,000 ohm.

FREQUENCY RANGE: 200 Hz to 10,000 Hz @ 3 db.

POWER LEVEL: 25 mW maximum.

LOW PASS FILTER: 30 KHz Cutoff. 40 db
attenuation in stopband noise. More than 70 db in
broadcast bands.

CONNECTORS: Output - Screw Terminal. Input -
0.14" Dia. miniature.

SIZE: 1 1/4" Dia. x 3 1/4".

WEIGHT: 3 oz. (85 gr.).

B.R. FOX COMPANY, INC.
EQUIPMENT SALES

1969 - 1971

*EQUIPMENT	PURCHASER	U.S.	States With	States Without
	Private	Government	Authorization	Authorization
	Enterprise		Statutes	Statutes
				(by state and quantity)
TS-125	0	0	0	0
TP-125	0	0	0	0
T-1200	0	0	0	0
T-1107	0	0	0	0
T-1104A	0	0	0	0
206	0	0	8	Miss.-1 La.-5 Ind.-1 Ohio-1 (8)
206CB	0	0	5	Miss.-1 Ind.-1 Ohio-1 La.-1 (4)
RB-101	0	0	5	La.-4 Ind.-1 (5)
600H	0	0	5	La.-3 Ind.-1 Ohio-1 (5)
X-800	0	0	0	0
272	0	0	0	0
275	0	0	0	0
312	0	0	0	0
701-X	0	0	5	Ind.-1 La.-2 (3)
355	0	0	0	0
201 201-D 201-E	0	0	6	La.-6 Ind.-1 Ohio-3 (10)
204	0	0	6	0
205 205-PA	0	0	5	Ind.-1 Ohio-1 (2)

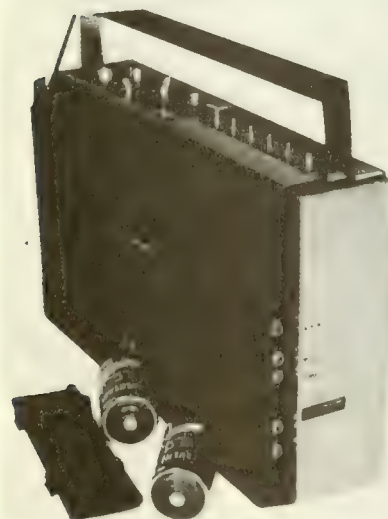
*For detailed description of equipment see attached advertisements

B.R. FOX COMPANY, INC.
EQUIPMENT SALES
1972 - 1974

*EQUIPMENT	PURCHASER Private Enterprise	** U.S. Government	States With Authorization Statutes	States Without Authorization Statutes (by state and quantity)
TS-125	0	0	1	0
TP-125	0	0	2	Mo.-1 (1)
T-1200	0	3	1	0
T-1107	0	0	0	0
T-1104A	0	0	1	Ind.-3 (3)
206	0	3	2	0
206CB	0	1	2	0
RB-101	0	0	1	0
600H	0	1	4	La.-4 (4)
X-800	0	0	2	0
272	0	0	0	0
275	0	0	0	0
312	0	0	0	0
701-X	0	0	3	0
355	0	0	0	0
201 201-D 201-E	0	0	1	0
204	0	0	2	0
205 205-PA	0	0	0	0

*For detailed description of equipment see attached advertisements

**Includes sales to DEA, CIA and Panama Canal Corporation



Item: CASSETTE RECORDER-RECEIVER COMBO
 Model: R-500
 Size: 2-1/2" x 12" x 8" (Approximate)

Comments: This is our most popular receiver unit. It is a standard, commercially available AM-FM radio, cassette recorder combination. The FM band has been modified in frequency yet the appearance of the unit has remained unchanged. A conversation may be monitored using this unit and at the same time be preserved on tape without the necessity for any patch cords and two or more separate units. It is portable or AC Line operated. The unit comes with a privacy earplug so that one may be standing on the street or sitting in the lobby of a building, use the earplug and remain completely discreet in all monitoring or investigative operations. The cassette recorder may be used separately without the receiver for other applications.

- ☐ This is the receiving unit to use with our Model T-275 Body Transmitter for a complete Transmitter-Receiver-Recorder System.

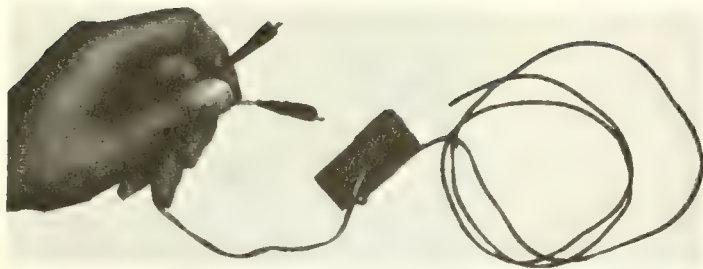


Item: AUTOMATIC TELEPHONE LINE TRANSMITTER
Model: TS-125 (Series Connected)
Size: 2" x 1" x 0.5"

Comments: This transmitter is connected in series on either the Tip or Ring side of the telephone line. It operates automatically, turning On when the telephone is in use, transmitting both sides of the conversation, as well as the number dialed on outgoing calls, to a receiver (such as the BRF #R-500 receiver/recorder), and turning Off when the phone is not in use.

No battery is needed with this unit as it operates off the existing power of the line. Once installed it is a permanent installation with no need to ever return. Undetectable to the user on the phone line. Could only be discovered by exact electronic measurement. Install at any access point such as a terminal box, telephone pole, or anywhere along the line.

Exceptional range of this unit makes it reliable in transmitting the conversation in any type area and gives clear distant pick-up even in congested situations. The unit is solid epoxied for rugged weather protection and is assembled with highest rating electronic components, for an unlimited lifetime due to its rigid construction standards.



Item: AUTOMATIC TELEPHONE LINE TRANSMITTER

Model: TP-125 (Parallel Connected)

Size: 2" x 1" x 0.5"

Comments: This transmitter is connected in parallel directly across the telephone pair without need to break the telephone line. It operates automatically, turning On when the telephone is in use, transmitting the number dialed on outgoing calls and both sides of the conversation, and turning OFF when the phone is hung up and not in use. It is designed to be used with the BRF #R-500 portable receiver/recorder as the receiving unit.

It contains its own battery power, so there is no drain from the telephone line making it undetectable even under telephone co. Central Office measurements. This gives it the highest security. Battery lifetime will give approximately 30 hours of actual telephone transmission. It is quickly installed at any access point along the telephone line.

The exceptional range of this unit makes it reliable in transmitting for long distances and gives clear reception even in congested downtown areas. The transmitter is solid epoxied for rugged weather protection, and it is assembled using highest rated, miniature electronic components, giving an unlimited lifetime to it due to these rigid construction standards.

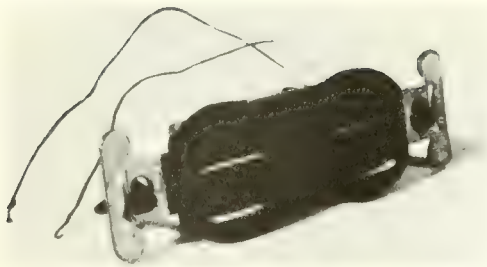


Item: AC WALL EXTENSION OUTLET TRANSMITTER
Model: T-1200

Size: Standard 3-outlet electrical extension plug

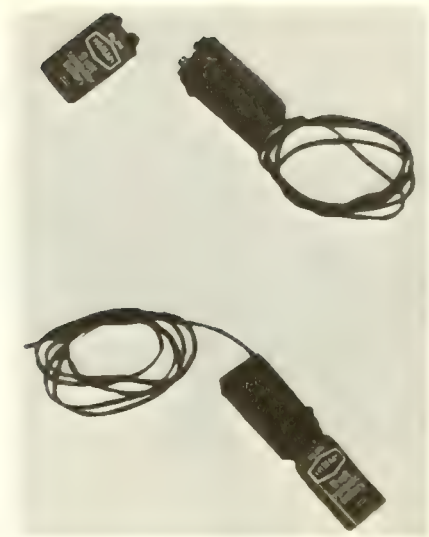
Comments: This device is perfect for those assignments that require the use of a concealed transmitter, do not offer time for an extended installation, and where later change of batteries is not possible. A miniature transmitter has been concealed in a standard 3-extension electrical outlet unit. All 3 outlets on this extension function as normal so that a lamp or whatever may be plugged into them. The transmitter is powered by the full 115 volts of the AC line, giving it an exceptional dependable range. It contains its own built in loaded antenna.

- ☐ This transmitter can be used with the BRF #R-500 portable receiver/recorder as the receiving unit.



Item: AC WALL OUTLET TRANSMITTER
Model: T-1107
Size: Standard electrical wall outlet unit

Comments: This device is a standard electrical wall plug receptacle which continues to operate as such, yet imbedded in the back is a powerful transmitter that is powered from the full 115 volt AC line voltage. Installation requires only access to the area, removing the existing receptacle, and rewiring this in its place, then putting the cover back on. The modification is completely unnoticeable unless the wall unit is again removed and inspected from the back side. Both plugs on the outlet function as normal, and the transmitter is activated continuously, or whenever the power is turned on to that receptacle, if, for example, it might be controlled by a wall switch. The ultra-sensitive sub-miniature microphone pickup assures complete coverage of any standard size room. A perfectly concealed installation with no battery concern once it is installed.

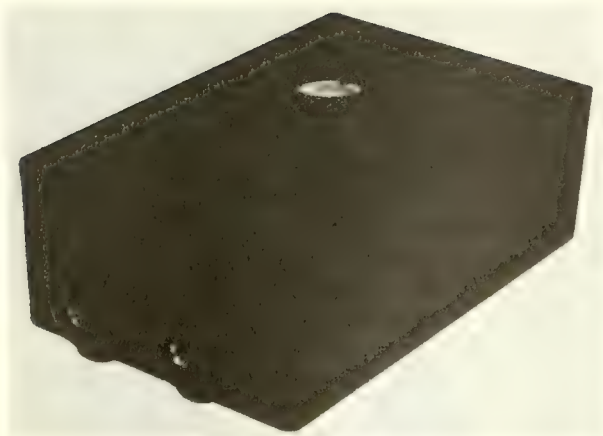


Item: MINIATURE DROP TRANSMITTER
Model: T-1104A
Size: 2" x 1" x 0.75" (Excludes its single 9v battery)

Comments: This miniature transmitter is designed to be dropped in a room, placed in furniture or stuck on the wall, and monitored from the outside. Its small size and sensitive, built-in mic, gives the ability to cover all room conversation with no involved installation time.

It is powered by a 9-volt radio battery (easily available), and will give approximately 18 hours of continuous transmission. For longer time periods, battery packs may be used connected to the same battery terminals of the transmitter. It is basically designed to be left in an area, but the unit can also be worn on the person as a body transmitter for close-in operations.

- ☐ Inexpensive, miniature, with sensitive mic and effective range. . .makes this a convenient tool in investigative operations.



Item: AUTOMOBILE SURVEILLANCE TRANSMITTERS
Model: T-301, Beep tone for tailing subject's auto
T-310, Audio transmitter for conversation within the car
Size: 3" x 2" x 0.5"

Comments: These units give continuous monitoring of either the conversation taking place within the automobile (Model T-310), or serve as tracking device by emitting a continuous beep from the subject's car (Model T-301).

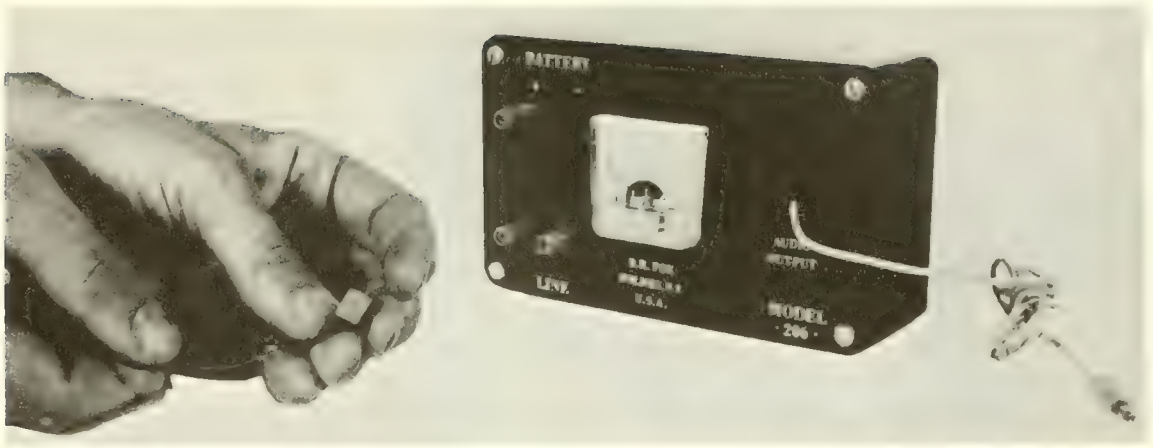
Installation is quick and easy. Insert the transmitter module behind the car radio by disconnecting the antenna cable from the rear connector of the radio and placing the transmitter unit between the antenna jack of the radio and the antenna cable of the auto. The standard connecting jacks are built in as a part of the transmitter unit. It operates off a positive 12 volt, negative ground system as exists on American and most foreign cars. The car antenna is used as this unit's transmitting antenna, with no interference with the antenna's normal function. A windshield antenna will make the surveillance transmitter's signal more directional, front to back.

Both of these models fill a vital need in automobile surveillance. . . .powerful transmission for long-distance coverage, with quick and simple installation. The transmitter's drain is negligible on the car battery and it can be connected permanently with no effects on the battery's operation.

The Model 310 unit transmitting the audio conversation from within the car must be used in conformance with the law enforcement restrictions on audio intercept of Title III of Public Law 90-351.

The Model 301 unit transmitting only a beep tone as a tailing device is not such an audio intercept device as Title III is directed.

Both units are designed to be used with the BRF #R-500 portable receiver/recorder as the receiving unit.



Item: SUB-MINIATURE MICROPHONE WITH INTEGRATED AUDIO PRE-AMPLIFIER
REMOTE CONTROL BOX FOR DISTANCE ACTIVATION UP TO 25 MILES

Model: 206 (Mic and Amplifier)
206-CB (Control Box at remote monitoring post)

Size: 3/8" x 1/4" x 1/4" (# 206)
6-1/4" x 3-3/4" x 2" (# 206-CB)

Comments: This system is unique in both its operation and its size. The smallest and most effective room "bug" developed. The ultra-miniature microphone has boosted sensitivity to voice frequencies. "Piggy-backed" on it is a deposited integrated pre-amplifier circuit containing 35 electronic components, which amplifies even the faintest conversation by 96 dB and send it out along Direct Wire, using a spare telephone pair or installed wiring, to the remote listening post. It is operative for distances up to 25 miles away between subject and listening post. No radiation of any carrier frequency gives the ultimate in security.

Its remote control box adjusts the sensitivity of the microphone with an easy meter reading on the control panel. Battery power is also supplied from the remote location via this control box. Its audio cable plugs directly into a speaker and/or tape recorder, such as the BRF # R-500, or BRF # 300 series reel-to-reel units for long term recordings.

One control box can activate any number of the #206 devices, but only one at a time. The # 206 mic can be installed anywhere within the area to be monitored, e.g. baseboard, telephone, connector blocks, etc., and it is then connected to a pair of conductors that are either already existing in the area or that have been laid. No need to ever return for battery change as it is all controlled from the listening end.

- ☐ The # 206 is solid epoxied with highest grade, sub-miniaturized and integrated electronic components. It has an unlimited lifetime.
- ☐ This is the most advanced device for permanent monitoring of an area in a maximum-security manner.



Item: CARBON MIC ACTIVATOR CONTROL BOX
Model: RB-101
Size: 6-1/4" x 3-3/4" x 2"

Comments: This unit will activate, and control the sensitivity of, any carbon microphone, such as that normally found in the mouthpiece of a telephone. Its special circuitry gives an ability to operate at distances up to 10 miles from the installation. It can thus turn the planted microphone On and Off, adjust its sensitivity, supply the battery power, and deliver the audio into a tape recorder all at a remote location. No need to ever return after the initial installation.

Any number of carbon microphones may be activated simultaneously when they are connected in parallel, and this control box will activate them all so that if the subject moves from one room to another there is continuous coverage.

Highest grade electronic components are used and the unit is solid epoxied to withstand rugged handling and provide an unlimited lifetime.



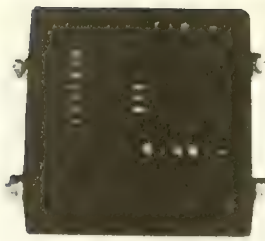
Item: AUTOMATIC TELEPHONE MONITOR
 Model: 600H
 Size: 6-1/4" x 3-3/4" x 2"

Comments: This is the most versatile automatic telephone unit available. . . use on a private residence phone, multi-pushbutton business phone, call-director set, entire switchboard, or coin telephone.

A tape recorder is turned On by this unit when the telephone is in use. The number dialed on outgoing calls, be it a rotary or touch-tone phone, is recorded along with both sides of the conversation. The recorder is automatically turned Off when the phone is not in use. Two plugs from the 600H connect directly into the audio input and the remote on-off jacks of the tape recorder.

This device not only monitors a single residence line, but is specially wired for use on a business multi-pushbutton phone set. In this application, it monitors whatever line is in use, and if that line is put on "Hold" it follows it there or onto a different line and then back to the original line. All conversation that goes out over that phone this unit will cover regardless what button is depressed at the time.

This device can be used to give the same automatic coverage of a pay telephone. It is compatible with the Bell System or any private telephone system, as might be encountered in some rural areas. The components are solid epoxied to give an unlimited lifetime of use. Tape recorder is not included. Specify make and model of recorder that is to be used, if possible, for correct impedance matching before shipment.



Item: TELEPHONE SLAVE UNIT
Model: X-800
Size: 3" x 1-1/4" x 1/2"

Comments: This latest development in direct wire remote coverage combines basic telephone operation with the most advanced electronic technology and miniaturization to give the ability to monitor a telephone line with distance to the listening post being no limitation.

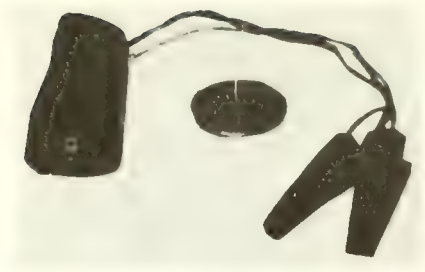
One side of the Slave is connected to the subject's line, the other side is connected to a leased line which you have had installed in the area, but with its telephone equipment removed and the number unpublished. The leased line is dialed in from the monitoring station wherever it happens to be, such as your office. The Slave automatically receives your call and connects you directly onto the subject's line. It is a one way connection, with all conversation on the subject's line being received at your listening station.

This unit can be used with the BRF #315 reel-to-reel recorder with voice activation for an automatic, long term recording coverage. The Slave can also be monitored manually. Any number of lines within a metropolitan area may all be wired into one control panel room and thus, for example, five operations may be conducted simultaneously and continuously from one central listening post. If any subject installation is outside the dialing area, an appropriate toll rate might apply, so, although a phone line in New York could be covered in Los Angeles, this installation is usually used within a local dialing area.

More extensive coverage could be obtained by using this Slave with the BRF # 272 which covers room conversation, automatically switches to the line when the phone is used, then switches back to the room when the phone is hung up. This entire coverage is achieved without being near the area.

- ☐ The Slave unit operates on all types of central office exchange systems, including the newest E.S.S. exchange equipment.

Solid epoxied to withstand all weather conditions and provide an unlimited lifetime of use.



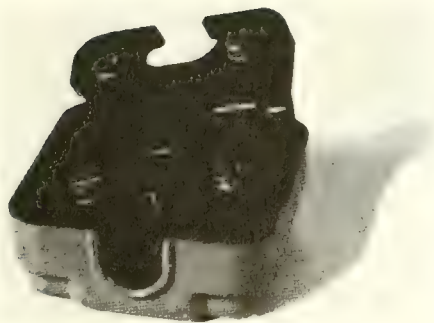
Item: COMBINATION ROOM AND TELEPHONE CONSTANT MONITOR
Model: 272
Size: 2" x 1" x 0.75", by itself,
or delivered concealed into a specific piece of telephone equipment,
such as a 42A connecting block (See Photo opposite page)

Comments: This little device provides a monitoring of any area in which it is installed, plus will automatically cover the telephone which serves that area. No extra wires are needed, other than the two (Tip and Ring) which activate the telephone.

The device is attached anywhere along the telephone line, in the telephone instrument, or at a connecting block. Its sensitive, sub-miniature microphone picks up all conversations within the area, gives booster amplification and delivers them out on the telephone line, without interfering with the normal telephone operation. The inside conversations are then monitored with the second part of the unit which is connected to the line at a convenient remote post. When the telephone is in use, the room monitor section AUTOMATICALLY disconnects and both sides of the telephone conversation can be monitored. . . . with the phone not in use, the room microphone picks up again. No batteries are needed so never a need to return once it is installed.

The information at the remote listening post can be plugged directly into a tape recorder for recording and/or monitoring. When used with the BRF Model 315 Voice—Actuated reel-to-reel tape recorder, it gives automatic recording operation with up to 9 hours recording time, with unattended coverage of both the room and its telephone.

When ordering, state whether unit is to be delivered as is, or molded into a specific piece of equipment. If it is to be concealed, the piece of equipment must be submitted with the order. In either form the device is constructed of highest-grade, sub-miniaturized electric components, all hand wired and molded in a solid chemical epoxy for an unlimited performance lifetime with proper handling and use.



Item: WALL MONITOR (Remote Dial-In Room Monitor)
Model: 275
Size: 2" x 2" x 0.9"
Delivered molded into a standard 42A connecting block
as shown in photo, unless specified otherwise by customer

Comments: Coverage of an area is now possible from a telephone at ANY location, be it local or long-distance. This unit is installed onto a telephone line in the area of interest. The telephone company would be instructed to install an unlisted number telephone line in the room, for example. The equipment is removed from the line, and this modified terminal block, which looks exactly like a standard one, is attached to the line. Its sub-miniature microphone is extremely sensitive to voice frequencies. It becomes activated when you dial this number, whether you are dialing from within the area, or from across the country. There is no ring, but the microphone circuitry is quietly activated so that you are in direct contact with the area and can hear whatever is taking place. In addition to its law enforcement surveillance applications, this unit is especially good for protecting industrial areas, where the owner can call in at any time during the night to check on his premises. Or use with a voice-activated recorder unit, such as the BRF Model # 315 for continuous automatic coverage. Special circuitry gives it the ability to have calling party disconnect. When the caller hangs up, the unit disconnects, so it is controlled by the person dialing into the number. . . . a number unknown to anyone but those privy to the operation.

- ☐ Concealed, discreet, and unlimited distant operation, with remote activation as easy as. . . well, dialing a telephone.



Item: REEL-TO-REEL RECORDER (3-Speed, up to 9 hours on one side)
Model: 310
Size: 15" x 7" x 12" Carrying case included

Comments: This recorder is excellent for use at the base station for long-term recording assignments. It handles up to a seven inch reel of tape and has a 3-speed selection: 7-1/2 i.p.s., 3-3/4 i.p.s., and 1-7/8 i.p.s. There is a separate volume control for monitoring while the recording is taking place, VU Meter indicator for incoming signals, and 4-position digital counter for easy tape reference. AC operation only.



Item: REEL-TO-REEL RECORDER WITH BUILT-IN AUTOMATIC TELEPHONE MONITOR
 Model: 312
 Size: 15" x 7" x 12" (Same as Model 310)

Comments: This is the same recorder as our Model 310 with all the features desired for a dependable base station recording capability. In addition it has a built-in network for automatic start and stop when connected to a telephone line. The connection is by means of direct wiring to the terminals on the back of the recorder. The switch on the recorder is then simply set to "AUTO" and the recorder will now start when the telephone is in use and stop when it is no longer in use.

- ☐ Extra Feature: The digits of a rotary dial telephone will be converted into distinct "beeps" and recorded on the tape so that the outgoing number being dialed can easily be determined by counting the clear "Beeps" on the tape. On a push-button dial phone, the tone of button depressed will be recorded on the tapes along with both sides of the conversation. 2-position switch provides use on standard telephone line or pay station phone.



Item: REEL-TO-REEL TAPE RECORDER WITH BUILT-IN VOICE ACTUATOR
Model: 315
Size: 15" x 7" x 12" (Same as BRF Model 310)

Comments: This is the same recorder as our Model 310 with a built-in voice actuator circuitry with direct connecting plugs on the rear of the recorder. By connecting the telephone line to the connectors on the recorder and putting the switch in "AUTO" position, the recorder will start automatically when there is voice conversation in the area being monitored or on the telephone line being monitored. The recorder will stop when the conversation has ceased. There is a sensitivity control to adjust the sensitivity level at which the recorder will turn on and off, and there is also a delay control to adjust the length of time the recorder will still continue running after the voice has terminated. When delivered from the factory this is set at 10 seconds with a nominal sensitivity setting. This Model 315 could be used with our Model 206 Miniature Room Pre-Amplifier, for example, and the system will give automatic i.e. unattended, room coverage. If used with our Model 272 room/telephone combo: it will give unattended coverage to both an area and the telephone line within that area.

- ☐ This modified recorder could also be used with the X-800 SLAVE for automatic operation of a remote telephone line monitoring system.
- ☐ The Fox 300-series of reel recorders provides a superior quality recording capability with both long-term coverage and automatic operation. They will give the finest recording at a base station in any investigative operation.



Item: TELEPHONE LINEMAN'S MODIFIED HANDSET
Model: 701-X

Standard telephone handset used by Telephone Company repairmen, with metal belt hook connector, and externally mounted battery and clip

Comments: This lineman's handset is essential for direct wire work on telephone systems. It is molded in heavy black rubber with ability to monitor or talk and dial on any active line terminal.

The modification has converted the standard unit to one having its own power source so that no power is drained from the telephone line, plus an extra stage of amplification. Complete silence when going across the terminals is the result. Absolutely no "clicks" or "pops" are heard on the line even if that line is in use at the moment the handset is connected across the terminals. Top Security with no compromise with this instrument.

- ☐ It contains a 3-position switch: Off, Talk or Dial, and Top Security Monitor



Item: CASSETTE RECORDER WITH CONCEALED TRANSMITTER AND
CONCEALED AUTOMATIC TELEPHONE MONITOR

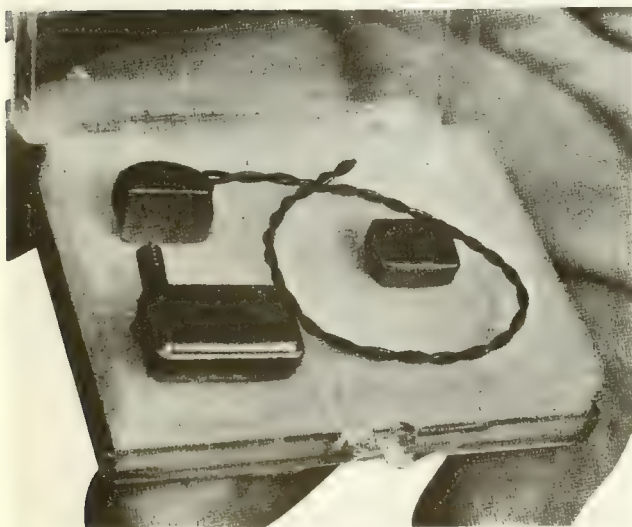
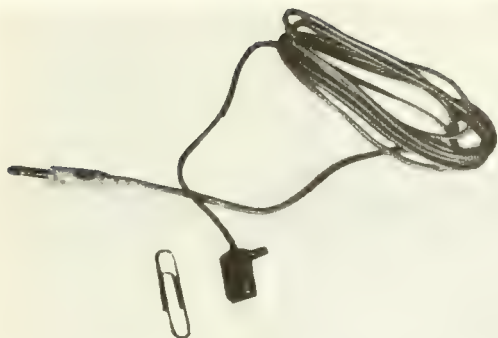
Model: 355

Size: 4" x 8" x 2" (Approximate)

Comments: This is a handy, top-quality cassette tape recorder with two concealed features which make it specially useful in investigative work. There is a built-in transmitter which is operated off the cassette's internal batteries. A micro-switch on the rear of the unit turns on the concealed transmitter. The unit may be sitting inconspicuously on a desk, in a bookcase, or elsewhere in an area while clearly transmitting all conversations within that area to a remote listening/recording post.

Also built-in to the unit is an automatic telephone monitor system. The normal AC Line plug has been converted so that when connected to a telephone line the cassette will automatically start when the telephone is in use and stop when the telephone is hung up, clearly recording both sides of the conversation and the outgoing number dialed. The cassette does not operate on AC Line voltage but on its own internal batteries.

This gives a useful cassette recording capability with two often needed investigative devices self-concealed within it.



Item: SUB-MINIATURE MICROPHONE
Model: 201 is sub-miniature dynamic microphone
 201-D is same as 201 with 36 inch lead terminated in phone plug for recorder input
 201-E is same as 201 with specified length of shielded cable up to 100 feet maximum terminated in a phone plug. (Add 7 cents per foot for shielded cable desired)

Comments: This intelligence microphone is specially designed to respond to the voice frequencies of interest. Its extremely small size makes it easily blend into existing room features. Pin-hole vent opening is smaller than the period at the end of this sentence. This dynamic microphone can be fed directly into a tape recorder. Available alone as a single unit or with 36 inches of shielded cable attached and terminated in a phone plug for direct input to a tape recorder.

Also available with any specified length of shielded cable attached, up to 100 feet maximum. Signal level at recorder input will decrease with increasing length of shielded cable.



(Shown next to paper match for size comparison)

Item: SUB-MINIATURE MICROPHONE WITH PLASTIC TUBING
Model: 204
Size: 3/8" x 1/4" x 1/4" (Approximately) with 12 inches of flexible accoustical tubing.

Comments: This is our 201 sub-miniature microphone with an extended vent opening to which is attached 12 inches of flexible accoustical tubing for easy "snaking" through small areas and avoidance of metal detectors. Its excellent accoustical response gives no reduction in microphone sensitivity. Designed for adjacent room use, e.g. under doors, through vents or outlets. Unit is supplied with sub-miniature microphone, 12 inches of flexible tubing attached, and 36 inch shielded cable attached to microphone, terminated in phone plug for direct input to tape recorder.

- ☐ If possible, specify make and model of tape recorder intended to be used for optimum impedance matching.



Item: CONCEALED SUB-MINIATURE MICROPHONE IN ELECTRICAL WALL OUTLET
Model: 205 Microphone in Wall Outlet only
205-PA Microphone with Integrated Circuit Pre-Amplifier
Imbedded in Electrical Wall Outlet
Size: Standard Electrical Wall Outlet

Comments: Our Model 201 sub-miniature microphone has been concealed within a standard electrical wall outlet to make our Model 205 and Model 205-PA. It is only necessary to gain access to the area, replace existing outlet with this specially modified one, "snake" the cable through the outlet leading into the adjacent room (these are usually mounted back-to-back) and replace the cover on the outlet. The sensitivity of the microphone will assure coverage of the room conversation. Both electrical outlets will function as normal. A completely disguised and effective device for concealed monitoring of any given area.

- ☐ Model 205-PA -- This modified wall outlet may also be ordered with our Model 206 sub-miniature microphone and audio-pre-amplifier installed in the electrical wall outlet. This gives maximum and controlled sensitivity from a remote listening post which may be in the adjacent room or could be at any point up to 25 miles away from the monitored area.



Item: MODIFIED AMERICAN TOURISTER ATTACHE CASE WITH
CONCEALED MICROPHONE AND EXTERNAL ON/OFF CONTROL

Model: 90-A

Size: 18" length x 3-1/2" wide

Comments: Smartly styled "slimline" attache case made by American Tourister, has a sub-miniature sensitive microphone concealed inside. Its pinhole opening in the grain of the finish gives discreet yet extremely sensitive pickup to cover entire room, automobile, or street conversations. Recorder is turned ON and OFF with movement of the normal open-close latch above the combination lock on the case. Most any recorder can be used in the attache case. The miniature cassette units can be inserted inside the closed compartment for undetected use even when the attache case is open. This also gives room for normal use of the case for paperwork. Its combination lock insures security when left unattended.

- ☐ Specify tan or grey attache case, and make and model of recorder to be used if possible, for an optimum impedance match of the recorder to the microphone.

Item: MODIFIED ATTACHE CASE, AS ABOVE, WITH PRE-AMPLIFIER MODULE INCLUDED

Model: 95-A

Size: Same as above

Comments: A high-gain, miniaturized integrated circuit pre-amplifier is included in this unit to give immediate amplification to the microphone's response. This produces an increased overall sensitivity in the unit so that distant voices can be recorded that would usually be missed with a straight mic into the recorder. This is the model to use for best sensitivity in reproducing the conversations picked up.

- ☐ Note: the tape recorder is not included in either of these units.

INTERVIEWS WITH MANUFACTURERS

Seven electronic surveillance equipment manufacturers answered the following questions in the course of interviews with the Commission staff. A summary of their responses follows each question.

1. How long have you been a manufacturer/distributor of electronic surveillance equipment?

The responses to this question ranged from 2 to 25 years. Four of the seven manufacturers were in business prior to Title III (Federal Wiretap Act) in 1968.

2. If in business prior to 1968, how have your sales been affected by the Title III legislation (primary consideration is volume and dollar value)?

Of the four manufacturers in business prior to Title III, three indicated a slight increase in law enforcement business, or at least in quality of equipment purchased, because of LEAA funding; one of these noted a drop in sales to industry and private investigators. The fourth indicated a drop in overall sales of prohibited equipment.

3. How many sales personnel do you employ, and what are their geographic responsibilities?

Three reported no sales personnel, all sales by mail or telephone.

One reported three sales personnel, one each in New York, Florida, California, but said most sales were by mail or telephone.

One reported six salesmen, all in the Southeastern U.S.

The last two reported seven and 12 salesmen, respectively, covering the entire U.S.

4. What information or training do you provide sales personnel with respect to the provisions of Title III?

Of the four employing sales personnel, the responses varied:

- provide a copy of Title III
- only hire those with law enforcement experience
- sell only to law enforcement personnel; thus no need for training
- 10 to 30 days of training on Title III laws; extensive training re police needs

5. How many manufacturing personnel do you employ?

Two employ none.

Four employ between 1 and 20.

One employs more than 150 manufacturing personnel.

6. Do you provide for the repair of electronic surveillance equipment?

All seven manufacturers answered yes:

- Six repair only their own equipment
- One repairs all electronic equipment

7. If so, what restrictions do you maintain to insure that the equipment is being possessed and transported in accordance with the law?

Generally require official letterhead if transaction is handled by mail, or personal identification if hand delivered, and the possessor is not already known to the manufacturer. One manufacturer criticized this part of the law as being vague and ambiguous.

8. What steps do you take to insure that the purchaser of your equipment is legally authorized to make such purchase?

Generally, by purchase order and letterhead of purchasing agency; sellers verify by contacting agency if there is any doubt. One manufacturer cited ambiguity in laws regarding sales to

states that don't have enabling legislation for Title III intercepts, noting "We do not police the police departments."

9. Do you require a written sales agreement?

Four stated that they do require such an agreement.

Three said they do not require a written agreement, although two of them encourage it, but will accept cable or even telephone orders as long as the equipment is to be shipped to an official address.

10. If so, what information is entered on such agreement?

Generally, name, address and equipment sold. Those who didn't require a written sales agreement prior to sale generally did require a follow-up purchase order or invoice.

11. What record keeping procedures are instituted with regard to sales?

Six reported keeping either invoice files or a card index of sales.

The Seventh keeps no record of sales, because he wouldn't want the information accessible to someone who shouldn't have it.

12. How do you advertise your electronic surveillance equipment?

Two do not advertise, although one of these responds to mail inquiries.

One does strictly oral advertising.

One mails directly to police departments, sends only a "teaser" for surreptitious equipment.

Three advertise in law enforcement magazines, but do not include Title III equipment; one of these stated that he had his advertisement approved by the Department of Justice before running it.

13. What procedure do you use in responding to outside requests for information (catalogues, etc.)?

Six answered that they respond only to requests from the law enforcement community on official letterhead; one of these added that he does not respond to inquiries from private investigators or foreign law enforcement agencies.

The seventh responds only to individuals he knows personally; all catalogues are personally delivered.

14. Do you display or demonstrate electronic surveillance equipment?

Six manufacturers answered that they did display or demonstrate equipment, generally at the request of the law enforcement community, either at the department facility or at conferences of law enforcement personnel. One expressed uneasiness at using a motel hospitality suite, presumably at such a conference, and indicated he had not held such a demonstration for the past five years.

15. If so, how do you transport the devices, and who are they shown to?

Of the six who do display or demonstrate:

- four have their salesmen transport the devices by hand.
- two expressed concern regarding the vagueness of the law, and indicated that they ship the devices by air to their own personnel.

16. How do you store electronic surveillance equipment?

Five responded that the limited amount that is stored is locked up and secured by guards and/or alarm systems.

One stores only on order.

One stores "just like any other, just like parts, right on the shelf."

17. What is your average delivery time?

Range of delivery time: 24 hours to 90 days.

Average: approximately two weeks to two months.

18. Who are your suppliers of electronic components (in the case of a distributor, the equipment supplier)?

Six of the respondents had suppliers:

- one had only one supplier
- three had 8-30 suppliers
- one had 1400 suppliers
- one obtained supplies from conventional radio supply houses.

19. Do you conduct training in the use of electronic surveillance equipment?

Six of the seven manufacturers/distributors reported that they do conduct such training. Four of those six hold the classes at the police department or training facility, a fifth holds them in a San Francisco hotel, and the sixth holds them at its own office. The training usually consists of demonstrations of use of electronic surveillance equipment, but there was great variation in the scope and length of training reported.

Five-day training is conducted quarterly by one company, but most conduct their training on a more flexible schedule. Generally, the training lasts several hours, but one company reported that it can be extended to a week or 10 days.

The choice of students is usually left up to the law enforcement agency involved, although one company limits attendance to members of the department directly involved in the use of the equipment. No special qualifications are required for students, and at least one of the manufacturers interviewed remarked on the general lack of knowledge of surveillance equipment on the part of many law enforcement officers.

Two of the companies reported keeping precise lists of those attending the classes, but the other four either kept no records or kept only records of cost or copies of invitations to teach, leaving the keeping of attendee lists up to the law enforcement agencies.

20. Do you sell electronic surveillance equipment to foreign governments?

Five of the seven answered no, two of them adding that the law is unreasonable and they would like to see it tested.

One answered that he very rarely makes such sales, and sells no surreptitious equipment.

One answered that he had not until recently, and that the Department of Justice was notified.

21. If so, what procedures do you use?

One ships the equipment as modules to be assembled on arrival.

22. How would you describe a device which is "primarily useful for the purpose of the surreptitious interception of wire or oral communications?"

—"A device which is not what it appears to be, i.e., lamp, furniture, etc."

—"Any device that records, transmits, or receives any kind of communication has that potential . . ."

—"Anything that can be placed in a room or area that will pick up the conversation of the people in that room or area . . . Anything that is attached to or in proximity of telephone lines and transmits the conversation of those lines to a receiver . . ."

—"A radio transmitter on a telephone line and received by a radio receiver at a distant point. A voice or room transmitter with best voice sensitivity when stationary and with range of twenty to thirty feet from it."

—"I don't believe that there is such a thing as a device 'primarily useful' for electronic surveillance, with the possible exception of the wireless transmitter."

—"Covertly used equipment. It depends on the individual—do you have an honest cop or a dishonest one? And how is he going to use it?"

—"The word 'primarily' is of no consequence and has no place in the law—it permits circumvention of Title III. It's for whatever the user wants to do with it."

23. Do you believe that manufacturers/distributors of electronic surveillance equipment should be licensed?

All responded affirmatively, one very strongly and three rather noncommittally.

24. Do you disagree with the relevant parts of Title III? If so, why?

One disagrees with Title III, feeling it is too restrictive economically.

All others agree generally with the intent of the statute but feel that it is too vague and could be considerably improved. Some of the specific criticisms included:

—should clarify, for example, whether manufacturers can deal with friendly countries. Are foreign embassies in Washington, D.C. classified as foreign shipments?

—too much variance in court decisions; too easily confused, "especially when you get some smart attorneys in court."

—"even working in this field I'm not sure whether I'm violating the law sometimes."

25. How would you improve Title III?

Definitions—

The improvement most frequently suggested was the clarification of Title III language, although there was not much indication of exactly how it should be done: "clarify definitions;" "clarify statute;" "better explanation regarding legality of use of equipment in specific instances."

Transport—

Four mentioned the confusion surrounding the transport and demonstration of equipment and suggested that that area be clarified; one suggested bonded carriers for transporting equipment.

Inventory—

Four suggested allowing manufacturers to inventory equipment, or perhaps only sub-assemblies, which could be strictly controlled (e.g., keeping running reports on what the manufacturer had in stock). Two others, however, recommended retaining the inventory restrictions, believing that relaxing the restrictions would lead to abuse.

Licensing—

Three recommended the licensing of manufacturers.

Export—

Two recommended removing the export prohibition.

Advertising—

One suggested allowing more liberal advertising, limited to specific publications. He argued that allowing limited solicitation of business would result in more competitive prices.

Training—

Various suggestions included: wider use of equipment and training of personnel; better training of law enforcement personnel; better definitions regarding training.

EXHIBIT NO. 3

FARGO COMPANY

1162 Bryant Street
San Francisco, Calif. 94103
Phone: Area Code (415)621-4471

June 5, 1975

Executive Director
National Wiretap Commission
1875 Connecticut Avenue, N.W.
Washington, D.C. 20009

Dear Sir:

The following information is submitted pursuant to your request for my views, as a manufacturer, of those aspects of the Federal Wiretap Act (18 U.S.C. 2510-20) with which I am familiar and with which I have had experience. You may enter this letter in the record of the hearings of your Commission if you desire.

At the outset, I would like to call the Commission's attention to the fact that Fargo Company, of which I am the founder and president, is the pioneer in providing audio surveillance equipment for law enforcement, having been continuously in operation since 1950.

I. Section 2512, Title 18.

By 1954 it became increasingly apparent from actual experience that not all persons would use surveillance devices legally and ethically. It became evident that there could be and was, misuse of equipment by non-law enforcement personnel that bordered on the illegal, or was actually criminal. Persons were using it for political and industrial espionage for either power, position, or profit. From actual experience we found that only law enforcement (city, county, state, federal, civilian, and military agencies, and friendly foreign governments) could be trusted to use this equipment properly. Because of this experience, in 1954, Fargo instituted a sales policy on its own initiative that any device that could be used for the violation of privacy would be sold only to law enforcement (totally tax supported) agencies. Fargo was the only company that had this policy for many years. In 1967 I testified at a closed hearing before the California State Assembly Criminal Justice Committee, and they agreed with my conclusions and passed a state law based on our sales policy. The Federal law, 2512, is quite similar to the California state law governing equipment, but is even more restrictive.

With the enactment of U.S. Code Title 18, Section 2512, by Congress in 1968, some interesting actions took place. Prior to the passage of this law, there was widespread distribution of clandestine eavesdropping devices to the public by over 100 companies. The Senate Sub-Committee on Criminal Practices and Procedures found that such devices were widely advertised in newspapers, magazines, electronics and Hi-Fi catalogs, and were widely sold in ordinary radio-TV stores. Within about a year, as the public and the manufacturers became aware of section 2512, the advertisements and devices in stores virtually disappeared from the market, and were thus not readily available to the civilian consumer. However, an interesting phenomenon occurred after Watergate in that these devices are again appearing in magazine ads and in stores, described as "babysitting devices", audio burglar alarms using miniature transmitters, and electronic secretaries (for wiretap instruments and recorders). Subminiature pocket recorders the size of cigarette packages are being marketed for conference recording or electronic notebooks. In the case of pocket recorders, a complex problem is presented, as the majority appear to be purchased for legitimate electronic notebooks rather than for any surreptitious use in recording another person's conversation. In this connection, I noted an ad from Playboy magazine, May, 1974, for a micro-mini mike transmitter not much larger than a paper clip. Also, the Lafayette Radio catalog showed a wiretap device that could be charged on BankAmericard.

Another question that section 2512 raises is: What happened to all the equipment that was in the hands of non-law enforcement personnel prior to 1968? Nothing has been heard of anyone destroying or getting rid of the equipment. What happened to the professional eavesdroppers who were doing private investigation work, and political and industrial espionage, who were so widely interviewed by the press, TV and other media, and used these interviews to further their reputations by this free advertising prior to passage of 2512? It appears that most went

underground, became careful as to who they selected as customers, but kept up their devious clandestine operations. Some later surfaced as "de-buggers" or "countermeasure technicians," sometimes as disguises for their actual activity, which was clandestine eavesdropping. It appears that very few went out of business.

The fact that eavesdropping devices are still being discovered in offices, on telephone poles, etc., supports a strong inference that professional clandestine eavesdropping for industrial and political espionage still exists. Because of the increased risks because of section 2512, these illegal operations were becoming extremely costly. Because of the secrecy of industrial/political eavesdropping, no one can say for sure just how widespread it is. However, it is interesting to note that of the devices that are discovered and make the newspapers (such as the H.L. Hunt case, Gordon Novell, etc.) most are accidentally found. The majority of the "finds" are usually kept confidential, especially in business. What corporate executive wants to admit to his stockholders that "the company was had" and perhaps cause the stockholders to get the impression that top management was lax in security in protecting their highly valuable company secrets? An interesting result of searches (countermeasure sweeps) made by competent, honest technicians reveals that only about 5% of the time are any devices found. However, this figure may not present an entirely true picture, as the eavesdropper may be tipped-off in advance by overhearing conversations by the targets that they might be "bugged," causing the eavesdropper to remove his equipment.

During the past ten years, Saber Laboratories, Inc., (specializing in detecting industrial electronic spying) has performed many countermeasure sweeps for the major industries in this country, and in only one instance was the sweep performed to detect what the customer thought might be government agency spying. All of the rest were for the sole purpose of detecting industrial spying.

It is my opinion that the threat today of industrial/political espionage, by the professional, illegal eavesdropper, using clandestine devices, is greater than it ever was. No laws are going to diminish his activity; they will only raise the cost for his services because of the increased risk. Only active, aggressive enforcement will stop him, and this is far easier said than done.

The detection of industrial/political spying has always been a very difficult, arduous task, with only limited successes. Most foreign spy operations involve networks that can be penetrated, but the industrial/political electronic spy works alone or with a partner, and detection is difficult, because all of his actions are carefully concealed and very secret. Section 2512 was, however, reasonably effective at stopping low level electronic eavesdropping, such as domestic (husband-wife, girl friend-boy friend, employer-employee, etc.).

Where do the professional eavesdroppers get their equipment? Most of them build their own devices, because it is no longer any major mystery how devices operate. Virtually any high school electronic student can build a basic eavesdropping device. Others purchase those thinly disguised devices advertised in magazines. As technology progresses, it is going to become increasingly difficult to distinguish between subminiature devices designed for strictly legitimate use and those that can be used for illegal eavesdropping. One of the prime goals of the electronics industry is the development of electronic equipment for legitimate commercial use that is smaller, lighter, and more powerful. Note the efforts of the tape recorder, TV, communications, and computer industries.

City, county, and state law enforcement agencies have slowly begun to take an interest in the responsibility that has been invested in them by state law in protecting the citizens' right of privacy. Two years ago, Fargo instituted a three day course in conjunction with John F. Kennedy University, Martinez, California, that is held three times a year here in San Francisco. This

course teaches law enforcement people their responsibility relative to illegal eavesdropping. It also teaches them how to conduct a countermeasure sweep, what to do in case of a "find," and report in writing in regard to electronic security hazards. The course covers both methods of how to conduct a countermeasure sweep, without equipment and with equipment. Over 75 law enforcement agencies have sent personnel for this training. However, considering the number of major law enforcement agencies, this is only a small percentage.

A very few agencies have even gone so far as to purchase countermeasure systems so that they can do a complete job. However, there are inherent problems for law enforcement agencies conducting sweeps, because they can only expect to be successful 5% of the time. Assuming the average survey (sweep) takes two men six hours each, or a total of 12 manhours, it would take an average of 240 manhours to find one device. It takes a lot of perseverance on the part of a technician to be so thorough he knows he has done a good job, and yet 95% of the time has only negative results to show for his efforts. This low ratio causes a morale problem.

While random efforts are made to discover the illegal devices, there has never been a major effort to discover and bring to justice the persons who are the professional eavesdroppers. In fact, prior to the 1968 Omnibus Crime Control Act, of which 18 U.S.C. 2512 was a part, professional eavesdroppers were actually glamorized by the news media. Conclusively, the threat of invasion of privacy of law abiding citizens by electronic devices today is not from law enforcement, but from their fellow citizens. In 24 years of selling surveillance devices to law enforcement agencies nationally, only on very rare occasions have I ever heard of a law enforcement man using this equipment for any reason except to bring criminals to justice. In most of the extremely rare occasions where law enforcement people acted illegally, the perpetrators were brought to justice by their own agency, or by another state or federal agency, with severe punishment because of the breach in trust.

Watergate had a profound but subtle effect on law enforcement when it was revealed that even the White House with all its influence and power, could not prevent a person from going to jail if he was caught using surveillance equipment illegally. This case, combined with a couple of other cases where police officers went to jail for violating the law on eavesdropping in the pursuit of criminals, caused knowledgeable officers to realize that when they performed an illegal act in the capture and conviction of a criminal, they risked:

1. Dismissal from the force.
2. Possible conviction and a jail sentence.
3. Forfeiture of their retirement benefits.
4. Disgrace for themselves and family.
5. Loss of their chosen career.

Friendly local courts or prosecutors might not be able to help. They would have the U.S. Department of Justice to contend with, as it is the enforcement body.

It is apparent that any law enforcement agent is going to think long and hard before he takes such a chance just to bring a criminal to justice. If he is caught, he can assume that he "has no friends," and not even a power as great as the White House can help. Of course, this restriction on law enforcement may benefit the criminal, who easily realizes that if he is in a state where wire or oral electronic interception by the police is prohibited, there is a good chance that his conversations and communications are free from interception, and this fact aids and increases his chance of a successful venture in crime.

An interesting aspect of the public's interest in what and how law enforcement uses electronic surveillance is the fact that for every piece of electronic equipment in the possession of law enforcement, there are at least 300 or more (a very conservative estimate) illegal pieces of equipment in the hands of the public that is not being used to apprehend criminals, the enemies of

society, but is being used by society against itself. There is little interest paid to the fact that this uncontrolled equipment is the real threat to society's right of privacy. There even seems to be some confusion in society's mind about making a clear cut distinction between the legal use of electronic surveillance equipment against the criminal and the illegal spying carried out by members of society against their fellow men in the interest of power, position, or profit at the expense of society's privacy.

II. "State of the Art."

The devices utilized by law enforcement today are not much different than those that were discussed before the Long Senate Sub-Committee in 1965-66, by various manufacturers. While they are smaller and more powerful, there has been very little change in the manner in which they are used with perhaps the exception of one device, the so-called "bumper-beeper." As it does not intercept oral or wire conversations, it may not even fall under section 2512. This device consists of a tiny black box mounted on magnets that sends out a beep tone. It is placed under a vehicle in seconds. It then permits a car equipped with direction-finding equipment to follow or locate the target vehicle, regardless of how carefully the driver of the target vehicle tries to conceal his whereabouts. Apparently these devices are available to anyone. They have good use in law enforcement, for legitimate "tailing" of criminals, and also for such businesses as the trucking industry to help the private security officer locate trucks that might be hijacked. What about the innocent person who wants privacy during his travels and takes elaborate precautions to be sure he is not "tailed"? If someone has placed a "bumper-beeper" on his car, it can easily be found, regardless of what extremes the target victim goes to conceal his path of travel. Is this a violation of his reasonable expectation of privacy?

Another device that has wide ramifications outside law enforcement is the PSE (Psychological Stress Evaluator). This is a chart device that attaches to a tape recorder and analyzes the changes (frequency modulation) of a voice and detects any stress changes that occur when a person lies. A person can be interviewed in public or called on the telephone. The taped interview or telephone call can then be easily analyzed by the PSE chart and the questions answered by lying can easily be discerned. As a law enforcement tool used under color of law, it is a valuable aid; however, what if an industrial spy or even a competitor calls a businessman and asks key questions about confidential company information? Naturally, the target is going to lie to protect his secrets. Yet the chart will show to what questions the answers are untruthful. These devices are sold without any government controls as to who has them and can use them.

III. Ramifications of Title 18, Section 2512, "Manufacture, distribution, possession, and advertising of wire or oral communication intercepting devices prohibited."

On the surface, to the manufacturer making these devices, the law is quite clear. However, the law makes two exceptions:

The first permits a communications common carrier, etc., to have such devices to maintain service. Example: The telephone company has the right to possess and use devices when it is done solely in the interest of maintaining good service. This exception has not, to the knowledge of the author, presented any problem.

The second exception permits the manufacture, distribution, or possession of such prohibited devices by "an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof . . ."

The Department of Justice, which is charged with enforcement of this law has made a very strict interpretation of it, as any

other approach would leave loopholes for unscrupulous persons or companies to take advantage of

To provide a better understanding of the Act and insure uniformity in construction, we discuss below a number of common misconceptions concerning these provisions of law. The first is the question of scope of authorized activities under the exceptions in 18 U.S.C. 2512. The exceptions do not permit advertising and do not permit transactions directly with foreign governments. The exceptions authorize only manufacture, distribution, and possession. Thus, a manufacturer may not publicly advertise prohibited devices, but circularizes only authorized purchasers. On the other hand, he may advise such purchasers that his firm is generally skilled in the production of electronic devices and respond to specific inquiries with information requested on prohibited devices. In addition a manufacturer may not maintain an inventory of assembled prohibited devices in anticipation of obtaining a contract with an excepted buyer, nor does a particular supplier's contract with an excepted purchaser legitimize another supplier's (dealer) transactions with the prime contractor. (Supplement No. 1, Department of Justice Memo 613, July 7, 1971)

The interpretation by the Department of Justice permits a person or company who has a valid (order) contract, which can be an official letter, purchase order, telegram, written contract, oral order or phone call (however, the manufacturer had better be able to prove by some acceptable means that he has received such a phone call or oral order) from one of the above listed agencies. Once the manufacturer has received such an order for a specific device, he can then proceed to manufacture the device for the agency, but only in quantities and exact type that the order calls for. If a manufacturer makes four devices and only has an order for three, and has the intention of putting the extra one in stock until he receives another order, he is in violation of the law.

The manufacturer cannot sell to an "individual" law enforcement officer with the power of arrest. However, an individual officer can order for his department if it is part of his prescribed duties. The transfer of ownership must be from the manufacturer directly to the agency qualified to purchase.

There is no prohibition on the types or number of devices a law enforcement agency can order. As title has to pass from the manufacturer to the law enforcement agency, sale to a dealer (or retailer, for example) who in turn resells to the agency is prohibited. It is permissible for a salesman or commissioned agent, designated by the manufacturer, to solicit contracts (orders) from qualified agencies. Equipment which has been ordered by a qualified agency can even be sent to the agent or salesman for demonstration to other law enforcement agencies, solely in the interest of soliciting an order or contract, prior to being shipped to its final destination. Manufacturers are prohibited from maintaining demonstration samples even though they are in the interest of soliciting a contract.

When a law enforcement agency wishes to "trade-in" a used device, the manufacturer may accept it as partial payment, but must have on hand a valid contract from another law enforcement agency for the "trade-in," or must immediately disassemble it to a state where it is no longer useful or easily made operable. Should he receive a qualified order at a future date, he is permitted to reassemble the device and sell to the law enforcement agency. Manufacturers are permitted to pay commissions to agents or salesmen of the company when they sell a device to law enforcement (but the salesman or agent must accept the order in the name of the manufacturer). Manufacturers are prohibited from advertising such devices in trade journals, newspapers, magazines, hand bills or TV. A manufacturer is permitted to print a catalog or brochure and use it to solicit contracts from qualified law enforcement agencies. These catalogs must be transferred by mail or other means directly to the law enforcement agencies. Putting them out at police conventions,

etc., is prohibited as well as display of actual working units of devices. The fact that a particular magazine may only go to police does not permit a manufacturer to insert an advertisement in it.

Should a manufacturer violate section 2512, his entire inventory of parts, etc., are subject to confiscation under section 2513 (seized and forfeited to the United States Government). Section 2512 also clearly mentions components of such a device, so a manufacturer cannot have any inventory of accessories that can be used for oral or wire communication interception. I refer to such components as wiretap adaptor, tube microphone, or other disguised microphones to be used with the device. A manufacturer of devices can carry a stock of spare parts, such as capacitors, transistors, plugs, etc. Here there is also an interesting interpretation: while parts themselves are not a device, when assembled they are the device. Therefore, should the part, previous to assembly, be made in another state, the device qualifies as having been in interstate commerce and subject to section 2512(b).

Section 2512 appears to prohibit the placing in, or advertising in magazines, etc., schematics, or plans and circuitry that permit the reader to assemble his own device. Section 2512 does not prohibit the showing of mock-up devices or devices that have been found in newspapers, TV, or movies, so long as the showing does not promote the use of them for sale to the public. Devices used by law enforcement against organized crime have been shown on TV, in books, newspapers, and in news items released to the press by law enforcement. However, if it were done by a manufacturer to promote sales, it would be prohibited. The manufacturers of devices sold to law enforcement automatically qualify themselves as having to adhere to section 2512 by the very wording of their catalogs or brochures.

Now, this is the grey area. There are manufacturers who are openly selling similar devices to the general public in stores, through magazines, etc. Most of them carefully word the description of the devices and are careful to avoid such words as "intelligence, secret, surveillance, audio interception, telephone tap" etc. They use words such as "silent monitor, intercom, babysitter, hot line" and, in the case of wiretap devices, "electronic recording secretaries." Here the question of intent arises and makes it difficult for the Department of Justice to enforce section 2512.

Almost every device that can be used for surreptitious interception of oral communications has more legitimate uses in industry than law enforcement. For example, the miniature pocket transmitter is far more widely used in motion pictures, TV, and the entertainment industry than it is in law enforcement. The hearing aid with its super sensitive amplifier, is a good eavesdropping device if you remove the subminiature microphone from it and connect it to a long, tiny wire. The miniature pocket recorder is also used by the businessman thousands of times for dictation of notes and letters. The problem becomes more complex every day from an enforcement standpoint.

One further point of interpretation of 2512 is the fact that section 2511 permits one-party consent interception (one person must be aware that the conversation is being recorded) but this does not permit a person other than law enforcement to possess a device that falls under 2512.

An additional problem is the telephone pickup coil for recording directly off the telephone, which is sold in almost every Hi-Fi, radio, and recorder shop in the country. Is this actually a device? There are probably 3 million or more in private hands today.

Further problems concerning the interpretation of section 2512: If a state, such as California, has a similar law, Federal law has precedence (California law permits the export of devices). If a state law is more restrictive, then the state law has precedence over Federal law. For example, if a state prohibits law enforcement officers of that state to possess devices, then the state law in regards to its city, county and state agencies has precedence.

IV. Surveillance "Binge."

Although the major emphasis has always been to guard against overzealous law enforcement surveillance, and although law enforcement uses it in its mission to protect society from crime and to apprehend criminals, law enforcement accounts for less than ten percent of all surveillance. One has only to walk into stores and see the myriad devices: two-way mirrors, closed circuit TV, special convex mirrors, etc. Then there are the business computers compiling files of personal information available to large groups of businessmen and others. Private detectives are available for hire to anyone for surveillance of another person; electronic and mechanical devices are available to check on our whereabouts or what we are doing. All types of night vision devices are used to penetrate darkness (available to the public); television cameras can see in the dark. This problem of controlling surveillance today is a problem that society has generated within itself because of its behavior patterns.

Whereas we have been concerned only with what law enforcement may do to violate our privacy, we are slowly reaching the point where we are going to be totally reliant on law enforcement to protect our right of privacy.

Society today is on a "surveillance binge," even to peepholes in our front doors, and like all "binges" it will be completely overdone, and it will eventually be law enforcement that will be actively enforcing antisurveillance laws. The Omnibus Crime Control Act was a step in the right direction.

V. Additional Observations.

There are about two dozen companies of relatively small size in the U.S. manufacturing various audio surveillance devices for law enforcement. The industry is actually rather small. The total dollar volume estimate is about a million and a half dollars, including all types of audio surveillance devices. However, as a conservative estimate, there are about 125 companies or persons manufacturing devices illegally, either knowingly or not realizing that such manufacture is illegal. They are selling to the commercial field, i.e., private investigators, security officers, private industry, industrial spies, etc. As these manufacturers do not print catalogs and often have other endeavors, such as TV repair shops, there is no accurate way of estimating the number of devices going into private hands (non-law enforcement).

Another unique aspect of law enforcement electronic surveillance is that in 24 years, Fargo Company has never found an honest law enforcement agency that was not firmly convinced that this was not only an invaluable tool, but absolutely essential, if a successful campaign is going to be waged against organized crime and major narcotic dealers. However, by the same token, it is very unusual to find a law enforcement officer who likes to do surveillance monitoring. It is a time consuming, boring job to have to listen to conversations in the hopes of picking up key words and phrases that will be useful in detecting the crimes to be, or that have been perpetrated. Electronic surveillance is actually diametrically opposed to the concepts of law enforcement that men choose as a profession. Surveillance monitoring brings little credit, and seldom any recognition because of its sensitive nature, to the law enforcement personnel who have to do the listening. Basically it is a thankless task for even the most sensitive crime information obtained. There are a number of cases on record where none of the agents wanted to do the actual monitoring, and it was done by the department clerks, and the case was lost on this point. In short, it becomes terribly boring work for personnel who wanted an active life in law enforcement. If audio surveillance were totally forbidden to law enforcement, it would not affect the job of a single law enforcement officer in the U.S. In fact, it could well have the effect of increasing major crime, which would result in the need for more police, which

would in turn require more supervisory personnel, thus making for more promotions within a law enforcement agency. This may be a strange philosophy, but nonetheless a fact of life.

Organized crime, like any business, requires rapid communications. The fact that they cannot trust their communication lines because of the threat of possible law enforcement interception has a definite limiting effect on their illegal activities.

While law enforcement agencies traditionally do not like to have outside supervision of their operations, they realize that it is essential to have supervision by the courts over electronic surveillance activities to assure the general public that we are not becoming a police state. So long as the courts, Congress, and the general public are concerned, and law enforcement keeps stating the need, we have a good healthy democratic climate. Should either side become complacent, we may be facing a loss of moral principles.

To further protect society, a time element might also be considered with regard to tapes of criminal investigations, notes, and transcripts of tapes made by law enforcement. Only relevant information should be kept. Once the information is no longer deemed essential, it should be purged from all records, and the tapes erased.

Some consideration should be given to more flexible laws to permit fast reaction by law enforcement to prevent such crimes as kidnapping and killings by dedicated radical groups that are politically oriented.

In times of relative peace and low crime rates, we should permit only the minimum use of audio surveillance. In times of great threat to public safety, permit limited expanded use on perhaps a geographic basis. For example, the threat today to the general public is very limited, say, in North Dakota, but is far greater in the San Francisco Bay Area of California (for example, the SLA and Zebra killings). Once the problem is overcome, then return to minimum standards.

Perhaps a study should be made of the effect of the California state law which does not permit recording or interception of any person's voice unless they are aware of it. The law does permit law enforcement to intercept so long as the law enforcement agency is party to the conversation.

With the advent of the subminiature recorders, it is comparatively easy to record the most private of conversations between individuals (by one of the participants). The Watergate tapes are the classic example of the unintended embarrassment that can result.

The telephone pickup coil is in wide use (probably a couple of million are in existence in the U.S.). The only true way of protecting the unsuspecting participant in a phone conversation from having his voice recorded surreptitiously (by telephone pickup or induction coil) by the other party is to require all participants to be warned at the beginning of the tape and agree to the recording, or to require a twenty second tone signal clearly audible on the telephone at all times when a recording is being made. However, such warning should not be required by law enforcement when investigating a criminal situation. With this type of law, the pickup coil would then be considered a surreptitious device under section 2512.

Bear in mind there can be extenuating circumstances when conversations are being recorded. It should not be illegal for a store owner to have a recorder concealed under his cash register counter with an activator switch to record a holdup, where the voice of the criminal is recorded for later identification by voiceprint. Special consideration should be given in these circumstances.

Sincerely yours,

FARGO COMPANY
[Signed]
Leo H. Jones

Pre-Title III Advertising - National Police Gazette, July 1967

ST

LISTENING DEVICES

EQUIPMENT FORMERLY AVAILABLE ONLY TO SECRET GOVERNMENT AGENCIES AND LAW ENFORCEMENT OFFICIALS

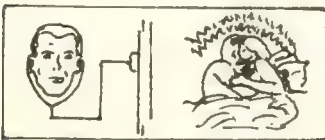


1. Subminiature "SONIC LISTENING BUG" can be easily concealed anywhere... behind a picture... under a chair or table! Will pick up the faintest sound in the room (even whispered conversations). Complete unit including instructions!

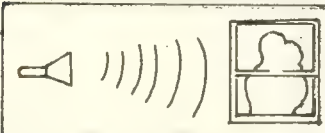


2. Super-Sensitive "TELEPHONE LISTENING DEVICE" picks up any telephone conversation! No connection to telephone necessary! You hear both sides of conversation from a distance, undetected! Complete unit including instructions!

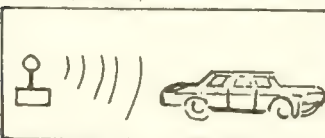
Complete instructions on how to make use of the following Electronic Listening Devices with minimum technical knowledge or skill necessary! COMPLETELY ALL NECESSARY PARTS!



A. Solid "WALL LISTENING DEVICE" which picks up conversations thru Solid Walls.



B. "Directional Microphone" which picks up conversations thru a CLOSED window 75 feet away!



C. "Car Listening Device" with which any auto can be bugged undetected!

FIRST TIME OFFERED TO PUBLIC!

For the first time in our many years of developing and manufacturing top secret listening devices for government and industry, we are making these very same devices available to the public! Electronic listening devices that formerly cost government and industry HUNDREDS OF DOLLARS EACH are now yours for just a FRACTION of their original cost!

YOU GET ALL THESE FANTASTIC LISTENING DEVICES!

- In this introductory offer you'll find:
- (1) A Subminiature "SONIC BUG" which can easily be concealed anywhere in a room and is so sensitive that it actually picks up the ticking of a wrist watch 50 feet away from the "bug".
 - (2) A Super-Sensitive "TELEPHONE LISTENING DEVICE" that will pick up both sides of any telephone conversation from a distance, and completely undetected!
- You'll also find simple, easy to follow, step by step instructions showing how you, in your very own home, with nothing more complicated than a screw driver, can make use of the following listening devices. We SUPPLY ALL NECESSARY PARTS and no technical knowledge or skill whatever is required!
- (A) An electronic "WALL LISTENING DEVICE" that enables you to overhear everything that occurs in any adjoining room or apartment!
 - (B) An ultra-sensitive "DIRECTIONAL MIKE" that will pick up what is up to 400 ft. away, and will even enable you to overhear complete conversations through a CLOSED window across an average size street!
 - (C) An electronic "BEEPER" which when placed in or

under an auto, transmits an easily traced superior signal, making it possible to follow the car at a safe distance without being detected.

UNBELIEVABLE NEW DEVELOPMENTS

But, that's not all! Directed to you is also found complete details on fantastic and unbelievable new developments in spying, eavesdropping, infiltration and subminiature recording equipment! Plus information on latest equipment designed for the DETECTION of eavesdropping devices. This unit is used in counter espionage by both government and industry!

WONDERFUL FUN! OR AN EXCITING NEW CAREER!

And finally, if you have ever thought of breaking into the investigation field, either creating your own small detective agency or working for the government or private industry, we include a complete course showing how you can make \$1000 - \$1500 per week in just your spare time, while you keep your present job. Once you have tasted the EXCITEMENT, ADVENTURE and BIG MONEY in this profession, you will soon devote full time to it!

10 DAY FREE TRIAL

Cut and mail coupon today! We ship same day order is received and you can examine the LISTENING DEVICES and INVESTIGATOR MANUAL in your own home for 10 full days. If you're not completely delighted and 100% satisfied, return unused equipment for a full and prompt refund of purchase price! NO QUESTIONS ASKED!

MAIL NO-RISK FREE TRIAL ORDER NOW!

ENCLOSE \$4.95 CONSIDERATION ADVANCEMENT PG-43 (302) WASHINGTON, D.C. 20001

Please return my LISTENING CRYPTOGRAPHIC DEVICES and INVESTIGATOR MANUAL. I will examine items in my home for 10 full days and if I am not 100% satisfied, I will return unused equipment for a full and prompt refund of purchase price.

NAME _____ CITY _____

ADDRESS _____ STATE _____

- ☐ I enclose \$4.95 Consideration Advance Payment post paid and shipping
- ☐ Send C.O.D. I will pay postman

TO MAKE AN EXTRA \$150 PER WEEK IN YOUR SPARE TIME!

BIG MONEY IN LISTENING DEVICES

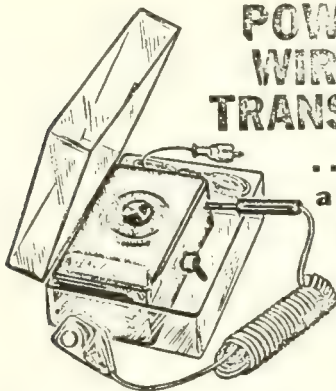
Copyright © A.

BIG DEMAND FOR MALE AND FEMALE INVESTIGATORS IN HANDLING ELECTRONIC LISTENING EQUIPMENT!

Do you like BIG MONEY and interesting work? EXCITEMENT and ADVENTURE?

You'll learn exactly how to:

- Pay a room - Top apartment
- Find, follow and intercept a car of a
- ADULTERY-EXTORTION - ROBBERY.
- See DEVIATION using electronic listening devices!
- Actual cost! And MUCH MUCH MORE!



POWERFUL WIRELESS TRANSMITTER

... the size of a package of cigarettes

ONLY \$12.95

Completely Assembled
Incl. 2 Microphones
& Battery

Here's a compact marvel of transistorized electronics that does just about everything... yet is tiny enough to fit in a pack of cigarettes. Called the WIRELESS BROADCASTER, this battery operated transmitter picks up sound through its sensitive microphone and transmits (without wires) thru any nearby AM radio. Unlimited applications:

- Broadcasting
- Guitar amplification
- Baby minding
- Remote Recording
- Sickroom Signal
- Auto to Home

This Really Modern Wonder Package comes completely assembled, and includes two microphones (1 Xtal for broadcasting, 1 contact type for musical instrument amplifying) plus a 9-volt battery. Fully guaranteed.

Send Cash, Check or Money Order to:

IMPERIAL ELECTRONICS Dept. PS-1

114 East 32nd. Street • New York, N.Y. 10016

44 | POPULAR SCIENCE

Popular Science - January 1968

POWERFUL WIRELESS TRANSMITTER

... the size of a package of cigarettes

ONLY

\$12.95

Completely Assembled
Incl. 2 Microphones & Battery

Here's a compact marvel of transistorized electronics that does just about everything... yet is tiny enough to fit in a pack of cigarettes. Called the WIRELESS BROADCASTER, this battery operated transmitter picks up sound through its sensitive microphone and transmits (without wires) thru any nearby AM radio. Unlimited applications:

- Broadcasting
- Guitar amplification
- Baby minding
- Remote Recording
- Sickroom Signal
- Auto to Home

This Really Modern Wonder Package includes two microphones (1 Xtal for broadcasting, 1 contact type for musical instrument amplifying) plus a 9-volt battery. Fully guar.

SUPER SLEUTH



This fantastic new private listening device has many applications, some of which we're sure you'll think of yourself.

- Help hard-of-hearing
- Hear TV Sound privately
- Amplify phone conversation
- Hear almost inaudible sounds
- 1001 Other Amplification Uses

Where do you want to listen in? The SUPER SLEUTH Audio Amplifier is powered by a single penlight cell (1.5V). 3-transistor circuit. Complete with output earpiece. Money back guarantee. Free catalog.

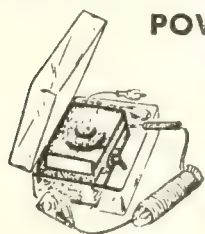
UNITS ARE COMPLETELY ASSEMBLED. NOTHING ELSE TO BUY!

BUY EITHER UNIT FOR \$12.95
OR 2 FOR \$23.95.

IMPERIAL ELECTRONICS,
DEPT. PS-11,

114 E. 32 St., New York, N.Y. 10016

Popular Science - November 1968



POWERFUL WIRELESS TRANSMITTER

... the size of a
package of cigarettes
ONLY \$12.95

Completely Assembled
Incl. 2 Microphones & Battery

Here's a compact marvel of transistorized electronics that does just about everything... yet is tiny enough to fit in a pack of cigarettes. Called the WIRELESS BROADCASTER, this battery operated transmitter picks up sound through its sensitive microphone and transmits (without wires) thru any nearby AM radio. Unlimited applications.

- Broadcasting
- Guitar amplification
- Baby minding
- Remote Recording
- Sickroom Signal
- Auto to Home

This Really Modern Wonder Package includes two microphones (1 Xtal for broadcasting, 1 contact type for musical instrument amplifying) plus a 9-volt battery. Fully guar.



SUPER SLEUTH

This fantastic new private listening device has many applications, some of which we're sure you'll think of yourself.

- Help hard-of-hearing
- Hear TV Sound privately
- Amplify phone conversation
- Hear almost inaudible sounds
- 1001 Other Amplification Uses

Where do you want to listen in? The SUPER SLEUTH Audio Snooper is powered by a single penlight cell (1.54). 3-transistor circuit. Complete with output earpiece. Money back guarantee. Free catalog.

BUY EITHER UNIT FOR \$12.95
OR 2 FOR \$23.95.

IMPERIAL ELECTRONICS,
DEPT. PS-9

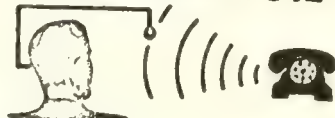
114 E. 32 St., New York, N.Y. 10016

UNITS ARE
COMPLETELY
ASSEMBLED.
NOTHING ELSE
TO BUY!

26 | POPULAR SCIENCE

Popular Science - September 1968

AMAZING NEW "LISTEN-IN-COIL"



PICKS UP ANY TELEPHONE CONVERSATION!

NO CONNECTION TO TELEPHONE NECESSARY! You hear the entire two way conversation from a distance... undetected! Limited supply remaining at only \$1.98. SUPER-SENSITIVE model \$2.98. Satisfaction Guaranteed! Catalog of LISTENING DEVICES 35c. FREE with order! Save COD fee and send Check, Cash or M.O. to: Consolidated Acoustics, DEPT 85, 1302 Washington, Hoboken, New Jersey.

Popular Science - January 1967



SECRET SNOOPER PICKS UP PHONE CALL

Amazing electronic DETECTIVE DEVICE! (Not sold where illegal.) Lets you monitor conversations undetected. Listen in on an extension without lifting receiver. Similar units sell for \$10. Now only \$2.98 while they last. WORLD CO., Dept. 11PS, 1 Park Ave., New York, N.Y. 10016

Popular Science - November 1968

TWO-IN-ONE ELECTRONIC MARVEL PHONE MONITOR & TELEPHONE AMPLIFIER

Can Be Used
With Phone on
Or Off Hook

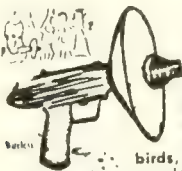
This minute size device used as a phone number affixes easily. By (no installation necessary) to the side of your extension phone and picks up conversations going through the main wire even without lifting the phone off the hook. As a phone amplifier with receiver off hook you can have a hands free conversation without being chained to your phone. This electronic wonder also enables you to listen in on hush hush conversation your teenager has. At the other, secretaries need to listen in without disturbing the conversation with expensive notes etc. Also a wonderful sound recorder when you, than one party wants to hear the conversation. Has volume control, operates on standard mercury battery (included) compatible with car plug. Only \$12.95 plus the up. Save \$2.00—two for \$24.95 p.p.d.



Send Check or M.O.
J. W. HOLST, INC.,

Satisfaction Guaranteed
Dept. PS-672, 1005 E. Bay St.
East Tawas, Mich. 48730

Popular Science - June & August 1972



Secret Listener

Hear Normal Talking 50 Feet Away! Hours of fun eavesdropping, hearing birds, animals, "night crawlers", even "noiseless sounds in dark! Styled after Army detectors, Point Reflector Sound Gathering "Gun" toward any sound. Big ear picks up, electronically amplifies and you listen thru 2 earphones. Easy to carry & conceal. Production made in Japan at amazing low price. Ruggedly made. In colorful gift box, ready to assemble and use in few minutes. Runs on hours on cheap trans. battery (35¢). About 10" long.

2570, Transistor
Electronic Sound Collector, Postpaid \$8.95
JOHNSON-SMITH, Dept. 267, Detroit, Mich.

Powerful, New, Transistorized Listening Device

SNOOPER-EAR

- Amplifies Sound
- Complete with Tripod & Earphones

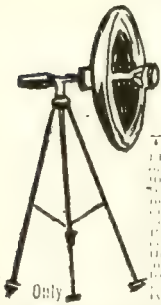
Electronic marvel. Works on same principle as fabulous Missile Tracking antennas. Aim disk reflector, hear jets roar in your special earphones. Pick up voices too distant to hear. Big 18" reflector-disc concentrates sound waves into the transistor unit and amplifies inaudible sounds loud and clear. Sturdy tripod with stethoscope-type earphones. Used by government agencies. Tape recorder can be plugged in. Fully guaranteed. **WORLD CO., Dept. 1PM, 1 Park Ave., N.Y.C. 10016.**

\$18.95
plus \$1.00
pp. & hdlg.



Popular Mechanics - March 1967

Popular Mechanics - January 1971



POWERFUL, NEW, TRANSISTORIZED LISTENING DEVICE SNOOPER-EAR Amplifies Sound

Complete with Tripod & Earphones. Electronic marvel. Works on same principle as fabulous Missile Tracking antennas. Aim disk reflector, hear jets roar in your special earphones. Pick up voices too distant to hear. Big 18" reflector-disc concentrates sound waves into the transistor unit and amplifies inaudible sounds loud and clear. Sturdy tripod with stethoscope-type earphones. Used by government agencies. Tape recorder can be plugged in. Fully guaranteed.

Only \$18.95 plus \$1.00 pp. & hdlg. Fully guaranteed.

THE BIG EAR

Powerful, New, Transistorized Listening Device

Only \$18.95
plus \$1.00
pp. & hdlg.

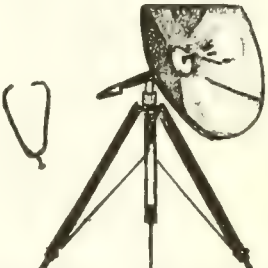


Tremendously Amplifies Sound

Complete with Tripod & Earphones

Here is the latest electronic marvel, right out of the space age. Signal corps model works on the same principle as the fabulous Missile Tracking antennas. Aim the disk reflector in the direction of high flying planes and hear the jets roar in your special earphones. Pick up conversations too distant for you to hear. The big 18" reflector-disc concentrates sound waves into the transistor unit and amplifies inaudible sounds loud and clear. Comes on a sturdy tripod with balance of aiming handle and is supplied with stethoscope-type earphones. Similar to units used by government agencies. Tape recorder can be plugged in.

WORLD CO., DEPT. IPS 1 PARK AVE., N.Y.C. 10016



TRANSISTORIZED LISTENING DEVICE. The "Big Ear" comes complete with tripod and earphones. Pick up conversations too distant to hear. 18" reflector-disc concentrates sound waves and amplifies inaudible sounds. Sturdy tripod with aiming handle, and stethoscope-type earphones. \$18.95 plus \$1.00 pp. & handling. World Co., Dept. PS-2, 1 Park Ave., New York, N.Y. 10016.

Powerful New Transistorized Listening Device

*SNOOPER-EAR

- Amplifies Sound
- Complete with Tripod & Earphones

Electronic marvel. Works on same principle as fabulous Missile Tracking antennas. Aim disk reflector, hear jets roar in your special earphones. Pick up voices too distant to hear. Big 18" reflector-disc concentrates sound waves into the transistor unit and amplifies inaudible sounds loud and clear. Sturdy tripod with stethoscope-type earphones. Used by government agencies. Tape recorder can be plugged in. Fully guaranteed.

\$18.95
Plus \$1.00
pp. & hdlg. Ave., N.Y.C. 10016.



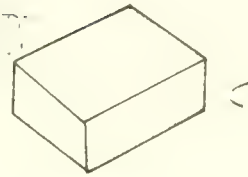
Popular Science - November 1968 through November 1971



Popular Science -
January 1968

MODEL 007 MICRO MINATURE WIRE TRANSMITTER

Radio Communications presents the Model 007 SECRET TRANSMITTER, the smallest commercially available radio broadcasting device utilizing the ultra space age technology. Sensitive enough to pick up a whisper across a large room, it transmits to any good FM radio with exceptional fidelity.



ACTUAL SIZE INCLUDING BATTERY

The system may be attached to any standard tape recorder, if desired. The transmitter's unusual reproduction qualities lend themselves to many other applications as well as surveillance work. For example, it is an excellent wireless microphone for use with a P.A. system or dictating machine. It thus lends well to monitoring sales presentations or conferences — or sounds from machinery, etc. Many other uses will suggest themselves, applications limited only by one's needs and imagination.

Security World - July/August 1967



Popular Science - November 1973

"Use as a silent monitor..."



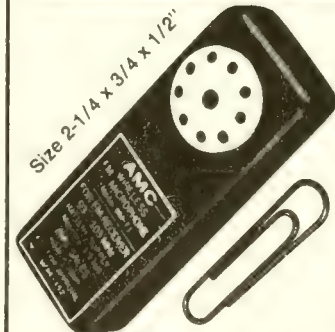
MICRO MINI MIKE WIRELESS

... Pick up & transmit
... eavesdrop without wires up to
... 400 ft. Use any FM radio, use as
... silent monitor, bug alarm, music,
... amplifier, intercom, baby sitter, hot
... line, etc. Comp. with BATT. Money
... back guarantee. Only \$14.95
... plus 50¢ for postage & handling.

AMC SALES, Dept. P Box 610, Downey, Ca. 90241

Playboy - May 1974

MINIATURE TRANSMITTER Wireless Microphone



Size 2-1/4 x 3/4 x 1/2"

Among world's smallest. Improved solid state design. Picks up and transmits most sounds without wires thru FM radio up to 300 ft. Use as mike, intercom, baby sitter, burglar alarm, hot line, etc. For fun, home and business. Batt. incl. Money back guar. B/A, M/C cds., COD ok. Only \$14.95 plus 50¢ Post and hdlg. AMC SALES, Dept. G, Box 610, Downey, Ca. 90241.

For Reader Service Information See Ad Index.

134 LAW & ORDER JANUARY 1975

Law & Order - January 1975

Saga Magazine - June 1970

WORLD'S SMALLEST TRANSMITTER!



LISTEN-IN ON ANY STANDARD FM RADIO!

This miniature electronic marvel picks up the slightest sounds and clearly transmits them to any standard FM radio up to 350 feet away! Latest engineering advances have reduced this unit to ONE HALF THE SIZE OF A REGULAR LENGTH CIGARETTE! Unit is completely self-contained including sensitive sub-miniature mike and battery!

This is the best performing transmitter that we have ever seen at anywhere near this low price. If you need a fine quality, low cost transmitter, this unit is for you!

SPECIFICATIONS:

TUNABLE: Between 88-108mcs.

RANGE: 350 feet

BATTERY: Mercury battery 1.3V
Mallory RM 675R

READY TO USE: Comes complete including battery and plastic screw-driver for changing frequency.

HUNDREDS OF USES!

WIRELESS MICROPHONE: For theatrical and TV productions.

SALESMANAGERS: Study and improve techniques of salesmen.

DRIVE-INS: Waitresses call in orders to kitchen.

INVENTORY: Check stock in plants and stores with stationary recorder.

PERSONAL BABY SITTER: Listen-in to sounds of baby from another room or yard.

GUITAR AMPLIFIER: Play any guitar or musical instrument thru FM radio, adjusting volume as needed.

BURGLAR ALARM: Be certain no intruders are entering home or business.

SALE PRICE **\$19⁹⁵**

MAIL NO-RISK FREE TRIAL COUPON NOW!

SEND NO MONEY—MAIL TODAY

SONIC DEVICES Inc. Dept. SA6
69-29 Queens Blvd.
Woodside, N. Y. 11377

Please rush me the WORLD'S SMALLEST TRANSMITTER! I will pay Postman \$19.95 plus small C.O.D. fee and I will examine the TRANSMITTER in the privacy of my home for 10 full days! If I am not 100% delighted and completely satisfied I may return the unit for a full and prompt refund! NO QUESTIONS ASKED!

Name

Address.....

City..... State..... Zip.....

☐ Check here if you wish to enclose check or money order and SONIC DEVICES, INC. will pay shipping charges.

Post Title III Advertising

"THE LITTLE BLACK BOX"

MINIATURE ONLY 122-12
ADD \$1.00 FOR SHIPPING
**SPECIAL SALE!
NOW ONLY
\$29.95**

WARNING! THIS DEVICE IS NOT TO BE USED FOR SURVEILLANCE!

AUTOMATICALLY STARTS RECORDER WHEN TELEPHONE IS PICKED UP. RECORDS ENTIRE TELEPHONE CONVERSATION. THEN, AUTOMATICALLY STOPS RECORDER WHEN TELEPHONE IS HUNG UP. CAN BE ATTACHED ANYWHERE ALONG THE LINE.

If you want to record both sides of any telephone conversation AUTOMATICALLY whenever a call comes in, this unit is for you!
This amazing device plugs into ANY cassette or reel to reel recorder and causes absolutely no interference or noise on the telephone.
Extremely useful around the HOME or OFFICE for making ACCURATE and PERMANENT record of all incoming and outgoing calls!

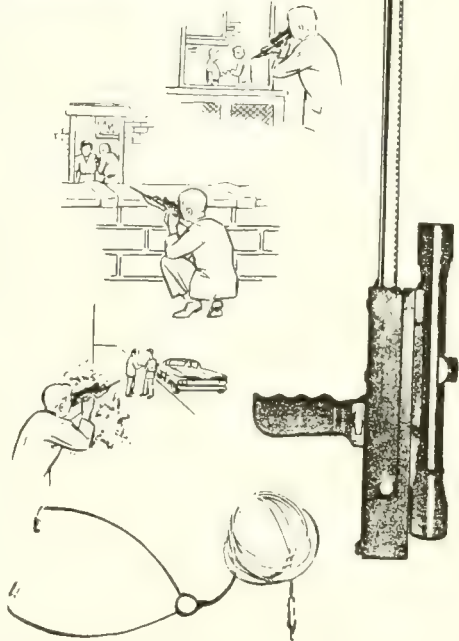
Shooting Times - March 1975

**HEAR
WHISPERED
SECRET
CONVERSATIONS****... thru SOLID WALLS**

NOW — With ordinary materials you can easily make a Super Directional Mike that amplifies sound 1,000 times. YES, YOU CAN ACTUALLY HEAR CONVERSATIONS THRU WALLS A BLOCK AWAY. Used by intelligence agents. So simple to make, that you will be using your Super Directional Mike 15 minutes after you obtain the ordinary store materials. Easy Instructions.

Only \$1.00 from: **SOUND WAVE, Dept. 6674**
6311 Yucca St., Hollywood, Calif. 90028

Saga Magazine - June 1970

**"GUN TYPE"
MICROPHONE**

The No. 902 "Gun Type" microphone is a portable, highly directional condenser microphone, complete with self-contained headphone amplifier, battery power supply, telescopic sight for aiming and visual surveillance of the sound source, and handgrip; can also be mounted on any standard photographic tripod

Specifications

Microphone: RF condenser type, impervious to air-pressure shock waves, humidity, mechanical vibration and electrical or magnetic fields; acoustic mode of operation is interference receiver, yielding a narrow frontal lobe (approx. 60° included angle) and a very high front-to-back ratio. Entirely solid state. Range: 100 to 300 feet, depending on surrounding acoustical conditions.

Amplifier: Entirely solid state, tailored for maximum response in the speech range; both microphone and amplifier operate from the same power supply

Power Supply: One 9-volt Duracell MB-1604 Alkaline Battery or equivalent

Headphones: Telex model HMY-2 or equivalent, 2000 ohms impedance, stethoscope type.

Dimensions: Length: 27" x 3 3/4" high (exclusive of hand grip) x 1 3/4" wide Weight 2 lbs 14 oz

FOR THE USE BY THE U.S. GOVERNMENT, STATE, AND THEIR SUBDIVISIONS
ONLY UNDER REGULATIONS PRESCRIBED BY P.L. 40-351

FAUROT
289 BROADWAY
NEW YORK, N.Y. 10007



DESIGNERS AND
MANUFACTURERS OF
DETECTION AND
IDENTIFICATION
EQUIPMENT

The Police Chief - Dec. 1971

1975 Advertisement

"KRYSTAL KITS"

P.O. Box 445

BENTONVILLE, ARKANSAS 72712

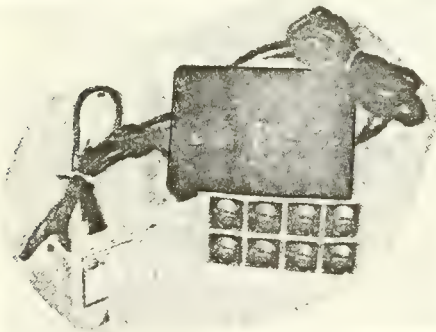
(501) 273-5340

OUR NEW ADDRESSOUR NEW ADDRESS

KRYSTAL KITS is a new company formed for the specific purpose to supply unusual and useful electronic projects in kit form for the hobbyist, experimenter, technician, and engineer, that are seldom found elsewhere. This does not say that our kits, supplied at our special low prices, are furnished with colorful step-by-step instructions similar to the ones that are furnished by the two major kit manufacturers. But we do supply first quality new component parts with a correct circuit diagram and helpful drawings to make the assembly an interesting and easy job for most any electronic enthusiast with a minimum experience in building up his own electronic projects.

All p.c. boards furnished with our kits are etched, drilled and are ready to use. It's our policy to refund your money if you are not completely satisfied with our products, provided the kit is returned within 10 days, unassembled and complete. As an added service, to our customers, KRYSTAL KITS offers construction and repair for any of our kits.

"AUTOMATIC ACTIVATED PHONE PATCH" Connect this solid-state adapter to your cassette recorder and telephone and you can automatically record all of your telephone calls without throwing a single switch. The AAPP must be used with a tape recorder that has a remote input jack; which most all recorders made today have. The AAPP operates by sensing the line condition, through a high impedance solid-state sensing circuit, without affecting or loading the telephone equipment, and this signal is converted to a drive current that is amplified and fed through a solid-state switch to turn on the recorder. The AAPP requires no battery or power supply to operate.



Complete kit of parts including a p.c. board (less plastic case); all you have to do is to add two plugs to match the mike and remote jacks on your recorder. Kit price is \$13.95 plus 50 cents postage.
Complete unit constructed and tested in cabinet only \$19.95 ppd.

PLANS FOR THE AAPP ONLY \$3.50 PPD.

"TELEPHONE AUDIO COUPLER" Transformer and coupling capacitor for matching the phone to your audio equipment without affecting the telephone equipment.
Kit price \$2.50 plus 25 cents postage.

"USE OUR NEW ADDRESS WHEN ORDERING FROM "KRYSTAL KITS"



**SECURITY
specialists
INC.**

WHEN YOUR JOB
GETS ROUGH. LET US PROVIDE
YOU WITH AN EXTRA MARGIN OF SAFETY!

BROCHURES AND DEMONSTRATION REQUESTS
MUST BE ON OFFICIAL DEPARTMENT LETTERHEAD!
P. O. BOX 3051 LANTANA, FLORIDA 33462

The materials on the following pages were received in the mail by one of the Commission investigators who responded to the following advertisement which appeared in the September 1974 issue of *Argosy Magazine*:

Wiretapping expose. Details \$1.00
(Refundable). Don-Q, Box 548-Y,
Seattle, Washington 98111.

The investigator had the materials sent to his home address and offered no official identification.

SUPER SENSITIVE

Ruby

FM TRANSMITTER

Super Sensitive FM Transmitter "RUBY" Model A-5 is an extremely small and compact FM transmitter that can be easily held in your hand. It clearly catches sounds at a distance of 100 to 200 meters. Apply it to a vast use by combining it with any FM radios in your present possession.

\$49⁰⁰



MODEL A-5.

Model A-5 is indispensable to:

- ① Directors, Sales Managers, Personnel Managers.
- ② Journalists, Advertisers, Marketing Researchers, Reporters, Stenographers.
- ③ Lawyers, Doctors, Teachers.
- ④ Information staffs, Private, detectives, Inquiry agencies.
- ⑤ Bankers, Bill Brokers, Frontmen.
- ⑥ Real Estate Dealers, Building Managers, Guardmen, Customer Service Managers.

APPLICATIONS

- ② Supervision or vigilance: No attendance supervision. Emergency warning. Supervision of sick-rooms or children rooms.
- ③ Moving Lectures: For lectures or speeches during movement as "RUBY" Model A-5 can be used as a high sensitivity wireless micropone.
- ④ Instructions or Command: Instructions against work process from remote site. Transmission of instructions to risky places, theater stages or distant and separated rooms.
- ⑤ Pursuit or Shadowing: Pursuit and supervision against moving objects.

FEATURES

- ① Small and light weight. Convenient in transport or carrying.
- ② High resistivity against shock or vibration. Permanently long life.
- ③ FM wave employed eliminates noise and assures a clear sonic quality.
- ④ Excellent sonic concentration. Its high sensitivity ensures perfect seizure of conversation at a distance of 10 to 15 meters. As Model A-5 is more sensitive than human ears, it clearly catches ticking of clock, intermittent dropping of water or whispering.
- ⑤ Covering Area: 100 to 200 meters in cities and 200 to 300 meters in suburb or in open field. As its wave penetrates concrete wall or floor, catching of conversation at 5 to 6 floors or rooms away in the concrete building or underground rooms is possible.

WALL HANGING THERMOMETER TYPE**NEW
PRODUCT!****FM TRANSMITTER****\$69⁵⁰**

CAUTION: This device is not offered for sale as a surveillance or spying device. It is illegal to use it for such purposes.

**MODEL TH-5.**

Wall hanging thermometer as you see is disguised into a super sensitive FM Transmitter as soon as a tiny battery is inserted into position. Its sensitive microphone catches all voices and sounds in the room, no matter how they are low and slight. It transmits an FM wave for more than a week. Whispering conversation in the room can be caught by an FM radio placed at 100 to 200 meters away. Model TH-5 is the most up-to-date weapon for

Model TH-5 looks as if a high class thermometer and will play a role of room accessory.

APPLICATIONS

When used in conjunction with the tone/sound activated mike - the ships wheel Fm Transmitter makes a fool proof undetectable perfect burglar proof device....Burglars are unaware they are being monitored and will expose themselves to you for easy apprehension...If used with tone mike and recorder a voice print can be further used for positive identification....

Can also be used for supervision of sick room or childs room.....

FEATURES

- ① Two in one set....highly finished wall hanger with thermometer plus sensitive FM transmitter.
- ② No one is aware of the mechanism even it is exposed to all eyes. Unless disassembled, inspection to internal mechanism is impossible if the rear lid is fastened with vise.
- ③ Excellent sonic concentration. Its high sensitivity ensures perfect seizure of conversation at a distance of 10 to 15 meters. As Model TH-5 is more sensitive than human ears, it clearly catches ticking of clock, intermittent dropping of water or whispering. A single unit of Model TH-5 catches conversation of 20 to 30 persons.
- ④ Covering Area: 100 to 200 meters in cities and 200 to 300 meters in suburb

SPECIFICATIONS

Modulation System :	FM (Frequency Modulation).
Oscillation Frequency :	To be specified one between 76 and 108 Mc.
Output Power :	4 mW.
Field Intensity :	15 μ V/m. at a distance of 100 meters.
Covering Area :	300 meters in open fields.
Transistors :	3, Micro-disc type.
Antenna :	Metal chain, 90 cm. long.
Microphone Unit :	Non-directional magnetic type.
Microphone Sensitivity :	-71 dB \pm 3 dB.
Frequency Characteristics :	\pm 7 dB at 500 to 5000 Hz.
Power Source :	Mercury battery "National Mallory" H-20/h (2.6 V) or equal.
Battery Life :	200 hours in continuous use.
Size :	65 mm. dia. in thermometer. 185 mm. dia. in wooden frame.

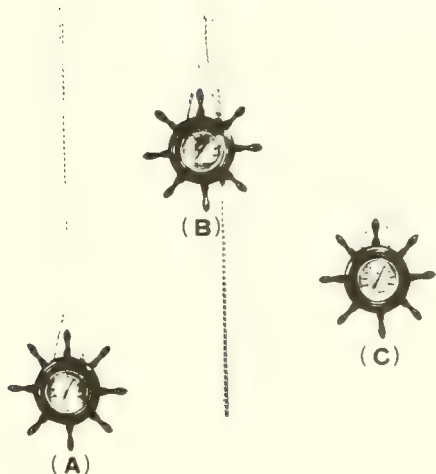
INSTRUCTIONS FOR USE

- ① As the metal chain plays a role of antenna of the transmitter, it should be hung down perpendicularly.

MODES OF HANGING:

- (A) The terminal of metal chain is hooked on a hanger on the wall and the transmitter is hung downward. This method is the best way to attain the most extensive range.
- (B) The chain is hooked at its middle part and the remaining length of chain is extended downward through the rear side of the transmitter. This method can be adopted if a covering area of only about 100 meters is required.
- (C) The chain may be cut at an adequate length if further narrower covering area is required. For example, for a covering area of 20 to 30 meters, the chain length required would be about 10 cm.

REMARKS: Please confirm before operation that the transmitter and its chain are perfectly standstill, as otherwise a disturbing noise may take place at the side of receiver.



- ② Insert the mercury battery into its position from the rear side of the transmitter. In doing so, be careful to the fact that polarities of mercury battery are inverse to those of ordinary batteries. In brief, the convex side (-) of the battery is inserted in the concave side the battery holder and the concave side (+) of the battery to the convex side of the battery holder.

- ③ Adjust the dial of the FM radio to match with the specified oscillation frequency of the FM Transmitter. Carry out a sonic adjustment by inserting the earphone into the FM radio as soon as a sharp "howling" sound can be heard.

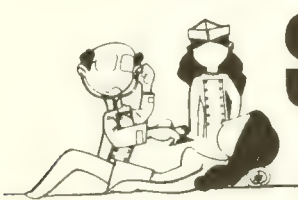
- ④ Any FM radios either portable, stereophonic or car radio may be used as a receiver. The higher the sensitivity, the more distant the wave spread.

- ⑤ For recording, the earphone jack of the FM radio and the input jack of tape-recorder are connected by means of the accessory cord. Then, the volume adjustment is made by monitoring the recording conditions.

- ⑥ The battery is to be removed when the transmitter is not in use.

HIGHLY SENSITIVE SPECIAL AUDIO AMPLIFIER SUPER STETHOSCOPE-ELECTRO

APPLICATIONS



1) Auscultation of human body. It plays a role as a stethoscope to pick up a slightest sound in human body.

\$6600



For guarding, management and prevention of crime. It can manage and guard acoustically unmanned rooms.

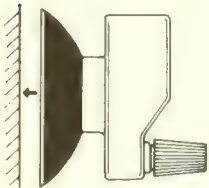
DESCRIPTION

RUBY Super Stethoscope-Electro is a highly sensitive special audio amplifier which can provide more precise and more correct data to technology in modern industries, such as architecture, civil engineering, machinery and so on. It can offer similar data to medical science, too. RUBY Super Stethoscope-Electro can amplify any sounds or voices by more than a thousand times.

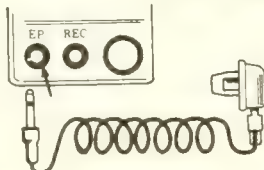
A rubber sucking cup enables adhesion to wall surface by pressure by hand and any voices or sounds can be heard through walls, doors or windows of glass, wood or mortar.

It can be connected to a tape-recorder.

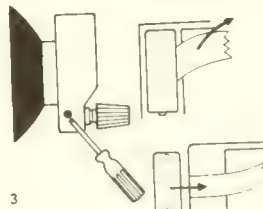
INSTRUCTIONS FOR USE.



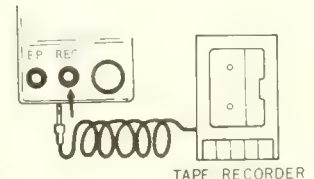
1



2



3



4

TAPE RECORDER

- 1) The unit may be attached to surface of any objects (glass windows, doors, walls, etc.) by means of the rubber sucking cup. Wet the cup slightly if necessary for better adhesion.
- 2) Plug the Ear Phone into the output receptacle marked reading "E.P." and fix the binner on the Ear Phone Tip. Rotate the Volume Control clockwise to switch the unit on. Then, continue to rotate the Volume Control slowly until a desired level of sound can be heard.
- 3) The solid-state amplifier in the unit is powered by one 1.5 volt ordinary small dry battery. Battery life is over 120 hours in continuous use.
Replacement of battery. Remove the back cover by unscrewing 2 screws and take a consumed battery out by pulling a ribbon prepared in the battery box. Insert a new battery in the battery holder as illustrated.
- 4) For recording, "REC" Jack in Model SM-11 and "MIC" Jack in a tape-recorder are connected with an accessory cable of tape-recorder.

CAUTION : Please be careful not to put this instrument into such a use which might infringe privacy of another person

	FIRST	SECOND	THIRD	FOURTH	FIFTH
TELEPHONE TRANSMITTERS	88-108 MHz (89 MHz)	60-85 MHz (71 MHz)	30-50 MHz (41 MHz)	108-120 MHz (110 MHz)	150-174 MHz (151 MHz)
ROOM TRANSMITTERS	88-108 MHz (89 MHz)	108-120 MHz (110 MHz)	60-85 MHz (71 MHz)	30-50 MHz (41 MHz)	BELOW AM BROADCAST
CAR TRANSMITTERS	88-108 MHz (89 MHz)	30-50 MHz (41 MHz)	27 MHz (CH 9)	60-85 MHz (71 MHz)	

*AM USING CONVENTIONAL CB TRANSCEIVER RECEIVER SECTION FOR MONITORING
 AM USING DETUNED AM RECEIVER OR 200 $\frac{1}{4}$ 500 KHZ LONGWAVE MONITOR

Preferred Frequency List

Where the radio eavesdroppers work and what frequencies they favor
 The most commonly-used bands for each of the three types of transmitters are listed in order of their preference (first to fifth) with the most often used frequencies for each band listed in parentheses below

The circuit diagrams described below present a fair cross section of the electronic transmitters being sold today. Like most on the market, they are not of sugar-cube size, nor are they the pre-1960 tube monstrosities. Those of you who may be electronic hobbyists might be interested in building some of them. Most can be constructed with readily-available parts and transistors designed for other applications and mass produced by the electronics industry. The result is that a good number of fairly sophisticated transmitters can be put together by anyone with a little knowledge of electronics for a grand total of less than \$21.00

PRICES OF SCHEMATICS INCLUDE..SCHEMATIC*PARTS LIST AND EXPLANATIONS OF UNITS.

1. UNDERSTANDING THE TELEPHONE OPERATION: PRICE \$3.00
 (a)..Three ways the telephone may be tapped
 (b)..The mechanical telephone.
 (c)..The electrical telephone
 (d)..Commercial telephones
 (e)..A basic telephone handset
 (f)..Telephone Transmitter operation
 (g)..Basic sound powered telephone

2. TUNNELL DIODE FM TRANSMITTER: PRICE \$3.00
 The TD(Tunnel Diode) FM Transmitter described in these plans is a very sensitive device, with about 50 milliwatts of output and range up to 300 yards, depending on receiving equipment.

3. A highly-sensitive Bug Detection field strength meter. PRICE \$1.00
 4. Simple Jammer will supply hash for room mikes. PRICE \$1.00
 5. Directional Receiver for pin-pointing the Bug-Loop-Detector has been designed for close work. PRICE \$2.00
 6. Bumper Beeper.(Can be heard easily up to 10 miles away on receiver equipped for continuous-wave reception. PRICE \$2.00

SCHEMATICS ONLY.....SCHEMATICS ONLY

7. Affectionately known in DE-BUGGING circles as the "LITTLE SCREAMER" This item combines sensitivity with output to ferret out hidden 88-108 MHz Transmitters. PRICE \$1.00
 8. AUDIO AMPLIFIER for a spike mike can easily be made small enough to insert in the wall or door with the microphone. PRICE \$1.00
 9. An experimental integrated-circuit radio telephone transmitter can transmit up to several hundred feet. PRICE \$1.00
 10. AM room transmitter built with tubes: Signals are stronger than those from most transistors..Also schematic for AM transmitter to operate in conjunction with the radio..2 schematics PRICE \$1.00

NOTE: IF ALL TEN (10) OF THE ABOVE SCHEMATICS ARE ORDERED AT ONE TIME,
 YOU MAY DISCOUNT FROM THE TOTAL PRICE OF THE ORDER A 30% DISCOUNT.
EXAMPLE.....TOTAL.....\$ 16.00
 Less discount 30%.....4.80
 Total you pay.....\$ 12.20

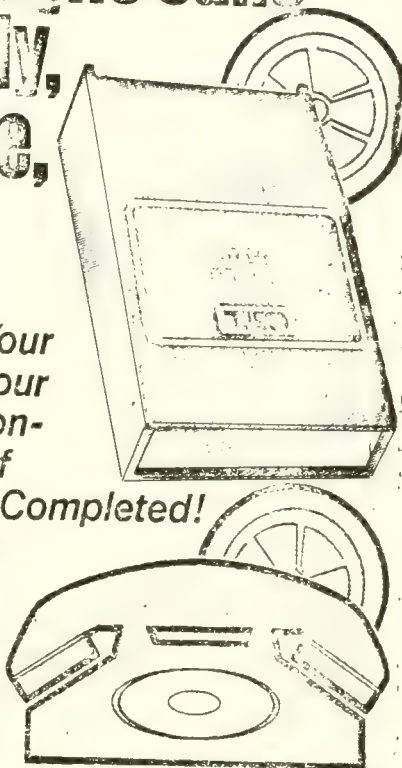
THERE ARE CERTAIN LAWS WHICH MAY PROHIBIT THE USE OF THESE DEVICES. IT IS THE SOLE RESPONSIBILITY OF THE BUILDER OR EXPERIMENTOR TO CHECK ON HOW THESE LAWS MAY APPLY AND TO NOT INFRINGE ON THE PRIVACY OF OTHERS.....

The following advertisement appeared in the New York Times on Nov. 30, 1974.

Now! Tape phone calls- automatically, undetectable, legally!

**New Electronic
Auto-Re-Cord Starts Your
Tape Recorder When Your
Telephone-Or Extension-
Is Picked Up...Shuts Off
Recorder When Call Is Completed!**

- Totally undetectable and silent
- Records off-premises extensions or answering service
- Use for dictation while away from office
- All solid-state/use with most standard portable tape recorders
- No interference with normal operation
- Use it at will — record some or all your calls. Simply plug into your tape recorder and phone line. The ATR-100 will automatically maintain a permanent record of some or all your phone conversations
- Can be installed anywhere
- Completely Automatic



JAY NORRIS 25 W. Merrick Rd.,
Freeport, N.Y. 11521
WAREHOUSE OUTLET
Come In Hours 9-5 (Mon. thru Sat.) (516) 546-8994
Serving Satisfied Customers for over 25 Years

Amazing Auto-Record connects easily to any phone to let you keep a permanent record of all your telephone conversations—at home or at the office! Automatically activates your tape recorder when your phone—or any extension on or off the premises—is lifted off the hook. Makes absolutely no sound—only you know that both you and person to whom you're speaking are actually being recorded! When phone is put back on cradle, Auto-Record immediately shuts off tape recorder.

Even works when an answering service takes your calls, so you can check the accuracy and thoroughness of your service's messages. Use Auto-Record for dictation when you're away from your office. Just call your secretary and let her put your message on tape for easy and accurate transcription!

Auto-Record creates no interference whatsoever with your phone's normal operation. Completely solid-state, it works with most standard portable tape recorders that run off batteries or AC Current. Simply plug Auto-Record into your recorder and phone line. Operates on just one regular 9-volt radio battery for an average of 6 full months!

So start "bugging" your own phone conversations! It's entirely legal—federal law requires that only one party in a phone conversation know the call is monitored—and you're the one in the know! Auto-Record is just \$29.99—order today! Order Now For Prompt Christmas Delivery.

ORDER BY MAIL WITH CONFIDENCE—
30-DAY MONEY-BACK GUARANTEE

JAY NORRIS WAREHOUSE OUTLET
25 W. Merrick Rd., Dept. AA-304
Freeport, N.Y. 11521

Please rush _____ Auto-Record(s)
\$29.99 plus \$2.00 shipping and handling
(1) SAVE! Order TWO for only \$56.00 plus
\$3.00 shipping and handling

Enclosed is () check or () money order
for \$ _____

Sorry, no C.O.D.'s—(N.Y. residents add
sales tax)

PRINT NAME _____

ADDRESS _____

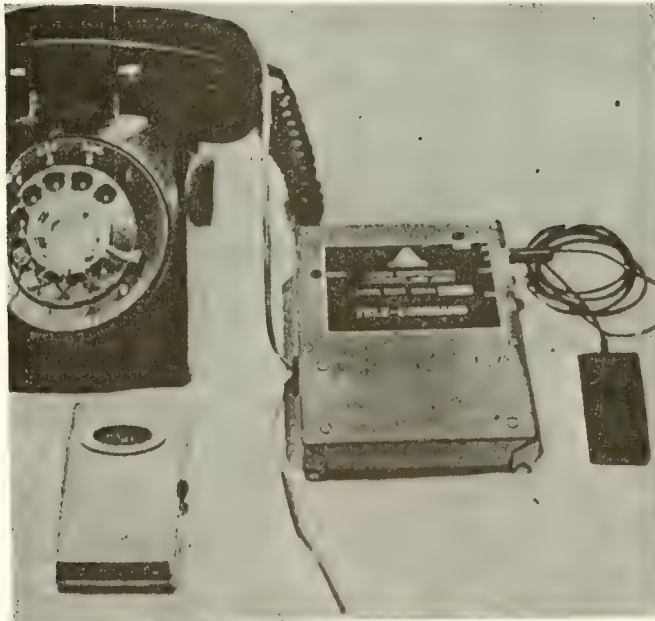
CITY _____

STATE _____

ZIP _____

© Jay Norris Corp. 1974

The devices shown on the following 3 pages are "burglar alarms" with listen-back capabilities.



Silent monitor that listens for prowlers★

Anybody in your home—who shouldn't be—when you're not there? With the Telecommand security system, you can phone and find out. It doesn't intercept calls, but listens in on the premises from a remote telephone. The system includes an audio amplifier and microphone in your home, and an interrogator you carry with you. Holding the interrogator to the mouthpiece while you dial activates the system without causing the receiving phone's bell to ring. A prowler won't even know he's being heard. Acron Corp., 1209 River Ave., Lakewood, N.J. 08701, makes the Telecommand.

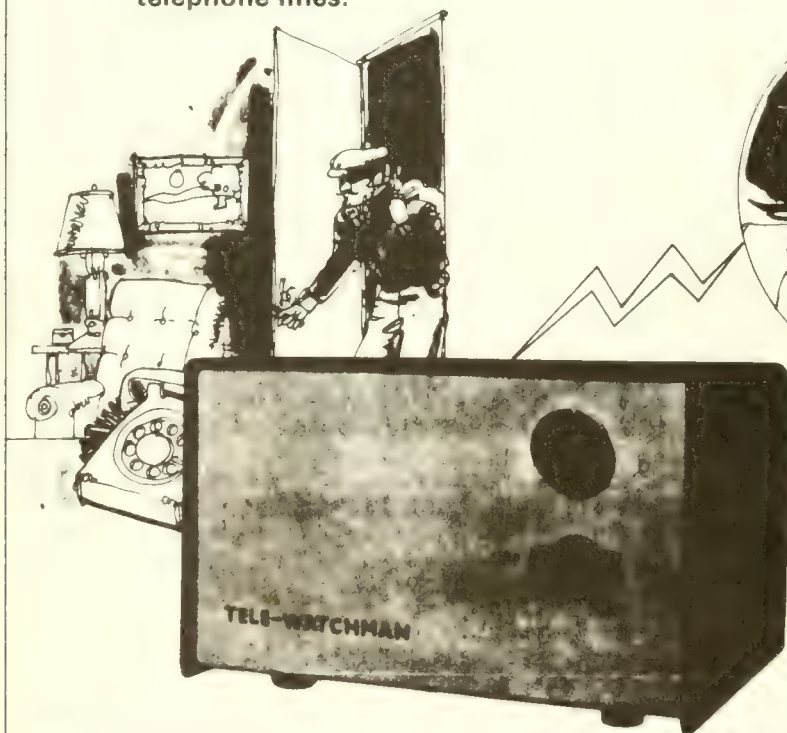
***the device that makes
the burglar alarm obsolete...***

THE TELE-WATCHMAN

it's new...simple...easy to install!

At last a burglar alarm that lets you monitor your premises at any hour.

The TELE-WATCHMAN offers inexpensive and quiet remote monitoring of offices, homes, stores, schools, plants, even cottages and boats via existing telephone lines.



For home or apartment residents who might normally fear surprising a thief or criminal on their premises, this device offers a safe and simple means of checking whether an intruder is present or not, at any time.

The unit operates from either 110 volt AC or it's own self-contained battery. Should power fail, the built-in battery takes over automatically, insuring continuous use. All components are reliable solid state.

Size: 6 x 5 x 4 ins. Weight: 2 lbs.

When installed and turned "ON" the TELE-WATCHMAN will automatically answer the phone without ringing and alerting an intruder. All sounds present in it's vicinity are then transmitted over the phone lines.

Even the most cunning intruder makes some noise. TELE-WATCHMAN's sensitive microphone can detect footsteps, whispered conversations, the rustling sound of paper, even the sound of striking a match.

With the help of our "MATCH-BOX", an accessory line matching device, the sounds can be recorded. The tapes may later be used as verification or identification by police.

The TELE-WATCHMAN is sold for the detection of burglaries, unauthorized entry and the prevention of crime only. No other use is intended, suggested or implied by the manufacturer, distributor or dealer.

With the use of a timer the TELE-WATCHMAN can be set to operate automatically within a certain period of time only. For example between 6 PM and 8 AM, leaving the phone line open for normal use during business hours.

Auxiliary jacks for additional microphones are provided. These may be placed in different locations, like plant, office, washroom, etc. In this manner several rooms can be monitored *ECONOMICALLY* with one unit.

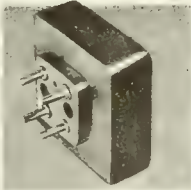
IDEAL LEASING ITEM FOR PROTECTION AND ALARM COMPANIES. SEVERAL INSTALLATIONS CAN BE MONITORED REMOTELY BY ONE PERSON.

\$199⁰⁰

"TELE-EAR" TELEPHONE ALARM MONITORING SYSTEM!

NOW YOU CAN CHECK YOUR PREMISES ANYTIME...FROM ANYWHERE!

CONSISTS OF:



The **TELE-EAR MONITOR** unit which plugs into standard telephone jack supplied with each system. This unit is placed at the site to be monitored.



The **TELE-EAR RECEIVER AMPLIFIER** unit which sits by your bedside telephone and continuously monitors your premises, even while you sleep!



The **TELE-EAR REMOTE ACTIVATOR** which will allow you to activate the **MONITOR UNIT** from any dial telephone.

CAN A BURGLAR DEFEAT THE TELE-EAR SYSTEM?

Absolutely impossible even if he cuts the telephone wires! Any cutting or disturbance of the telephone line immediately breaks the telephone circuit between telephones and results in a shrill warning tone (actually the dial tone amplified about 50 times) emitted from your **RECEIVER AMPLIFIER**!

WHAT ABOUT FALSE ALARMS?

Again impossible! Any noise that you hear will actually be occurring as you hear it. If you are not completely certain as to what caused the sound, a little careful additional listening will quickly reveal its source! A burglar will not stand still. If he thinks he is undetected, he will continue about his job making additional sounds that will surely give his presence away!

A QUICK CALL TO THE POLICE WILL INvariably CATCH HIM IN THE ACT!



HERE'S HOW IT WORKS!

As you dial the last digit of your business telephone number, hold the **REMOTE ACTIVATOR** close to mouthpiece of telephone. A special frequency tone will instantly activate the **TELE-EAR MONITOR** at the site being called! The telephone will not ring and any and all sounds at your business site will now be clearly heard on the telephone.

If you are calling from your home, simply turn on the **TELE-EAR RECEIVER AMPLIFIER** unit and hang up your telephone! You can now sleep peacefully... completely secure in the knowledge that you will be instantly awakened by the slightest disturbance at the site being monitored!

THE TELEPHONE NEVER RINGS!

YOU WON'T ALERT A BURGLAR BY A RINGING PHONE! The telephone in your office or business will not make the slightest sound! It will sit there just as innocently as ever... WHILE YOU SAFELY MONITOR THE PREMISES!

WARNING!

THE TELE-EAR IS NOT A "BUG"!

Because the very nature of this fantastic device makes it possible to monitor areas without observance, we must point out that federal law permits the use of the **TELE-EAR ONLY** as a burglar alarm.

It is illegal to use the **TELE-EAR** to surreptitiously monitor the conversations of parties that are unaware of its presence!

H. L. B. SECURITY ELECTRONICS, LTD.

211 EAST 43RD STREET, NEW YORK, NEW YORK 10017
(212) 986-1367

Licensing Requirements for Manufacturers and Sellers of
Electronic Surveillance Equipment under the Canadian Protection of
Privacy Act, Section 178.18 of the Criminal Code

Under this law, a sponsor (e.g., Chief of Police, Director of Criminal Investigation, head of a branch of government) must write a letter to the prospective licensee authorizing the possession/manufacture/sale of "enabling devices" ("electromagnetic, acoustic, mechanical or other device or any component thereof...primarily useful for surreptitious interception of private communications") on the sponsor's behalf. The licensee must then fill out an application and forward it with letter(s) of endorsement from sponsor(s) to the Registrar (Commissioner of the Royal Canadian Mounted Police).

The license authorizes possession/manufacture/sale between the licensee and his sponsor only, and is limited to the express conditions therein. The licensee shall not possess/manufacture/sell such devices except under specific authority from his sponsor (or in the case of a special license, from the Registrar) for each transaction.

A license may be revoked by the Registrar upon the licensee's failure to observe its terms and conditions, which include: reporting within 10 days any change in the information shown on the application; producing the license to a police officer on demand; and storing the devices in such a manner that they will be inaccessible to the public.

Except in the case of special authorization by the Registrar, the license will expire on the date indicated on the license unless the licensee applies for its renewal not less than 30 days prior to the expiration date; any such application must include a new letter of endorsement from a sponsor. If an endorsement by a sponsor is withdrawn during the term of the license, the Registrar will revoke the license and give written notice of the revocation to the licensee.

TERMS AND CONDITIONS

CONDITIONS

1. In these terms and conditions
 "authority to purchase" means a letter written by a sponsor to his licensee authorizing the licensee to possess (including if applicable to manufacture) and/or sell enabling devices on the sponsor's behalf.
 "enabling device" means an "electromagnetic, acoustic, mechanical or other device" as referred to in section 178.18 (1) of the Criminal Code.
 "letter of endorsement" means a letter written by a sponsor who is in lawful authority over persons who may lawfully possess enabling devices under section 178.18 (2) (a) and (c) of the Criminal Code.
 "Licence" means a licence issued pursuant to section 178.18 (2) (d) of the Criminal Code.
 "licensee" means a person in possession of a licence.
 "Registrar" means the Commissioner of the Royal Canadian Mounted Police.
 "special licence" means a licence issued without the requirement of a sponsor.
 "sponsor" means the Chief of Police of an accredited police force, the Director of Criminal Investigation, the Director General, Security Service, or Commanding Officers of any Division of the Royal Canadian Mounted Police, the Commissioner of the Ontario Provincial Police, the Director General of the Quebec Police Force, the Director General Intelligence and Security of the Canadian Forces and in the case of an officer or servant of Her Majesty in right of Canada, the head of the branch of government that employs him or of which he is an official.
 2. This licence authorizes possession (including if applicable to manufacture) and/or sale of enabling devices between the licensee and his sponsor only and shall not be construed as being a general licence to possess (including if applicable to manufacture) and/or sell enabling devices.
 3. Possession (including if applicable to manufacture) and/or sale of enabling devices under a special licence shall be limited to the express conditions set out therein.
 4. The licensee shall not possess (including if applicable to manufacture) and/or sell enabling devices except under specific authority to purchase for each transaction from his sponsor or in the case of a special licence from the Registrar.
 5. Enabling devices in possession of a licensee shall be secured in such a way that the public does not have access.
 6. The licensee shall report any change in the information shown on the application form for a licence to the Registrar within 10 days of such change and further the licensee shall report such information as the Registrar may from time to time require.
 7. The licensee shall produce his licence to a peace officer for inspection upon demand, together with the authority to purchase for enabling devices in his possession or in a state of manufacture.
 8. If an endorsement by a sponsor is withdrawn, the Registrar will revoke the relevant licence and give written notice thereof to the licensee.
 9. A licence may be revoked by the Registrar upon failure of the licensee to observe its terms and conditions.
 10. Except whereas directed otherwise and endorsed by the Registrar the licence will expire as indicated by the expiry date on the licence unless the licensee applies for its renewal not less than thirty days prior to such expiry date.
 11. An application for renewal must be accompanied by a new letter of endorsement.
 12. Special Terms and Conditions.
1. Dans le présent contexte,
 "permission d'achat" signifie une lettre rédigée par un répondant, à l'intention du détenteur et l'autorisant à posséder (à fabriquer, s'il y a lieu) et à vendre des dispositifs d'interception au nom du répondant;
 "dispositif d'interception" désigne "un dispositif électromagnétique, acoustique, mécanique ou autre", tel que mentionné au paragraphe 178.18 (1) du Code criminel;
 "lettre du répondant" désigne une lettre rédigée par une personne qui a charge légale de personnes autorisées à avoir en leur possession des dispositifs d'interception en vertu des alinéas 178.18 (2) a) et c) du Code criminel;
 "permis" désigne un permis délivré en vertu de l'alinéa 178.18 (2)d) du Code criminel;
 "détenteur" désigne une personne qui possède un permis;
 "régistrare" désigne le commissaire de la Gendarmerie royale du Canada;
 "permis spécial" désigne un permis délivré sans que celui qui en fait la demande ait besoin d'un répondant;
 "répondant" désigne le chef d'un service de police reconnu, le directeur de la Sûreté, le directeur général du Service de sécurité, les commandants divisionnaires de n'importe quelle division de la Gendarmerie royale du Canada, le commissaire de la Sûreté de l'Ontario, le directeur général de la Sûreté du Québec, le directeur général des renseignements et de la sécurité des Forces armées canadiennes et, dans le cas d'un fonctionnaire ou préposé de Sa Majesté du chef du Canada, le chef de la direction du gouvernement qui l'emploi ou dont il est un fonctionnaire.
 2. Le présent permis autorise la possession (la fabrication, s'il y a lieu) et la vente de dispositifs d'interception à l'égard du détenteur et de son répondant seulement et il ne devrait pas être considéré comme un permis général de possession (de fabrication, s'il y a lieu) et de vente desdits dispositifs.
 3. La possession (la fabrication, s'il y a lieu) et la vente de dispositifs d'interception en vertu d'un permis spécial ne sont autorisées que suivant les conditions expressément mentionnées.
 4. Le détenteur ne doit pas posséder (fabriquer, s'il y a lieu) et vendre des dispositifs d'interception sans une permission spéciale d'achat de son répondant pour chaque transaction, ou, dans le cas d'un permis spécial, sans une autorisation spéciale du registraire.
 5. Les dispositifs d'interception en la possession d'un détenteur doivent être rangés dans des endroits sûrs, et de telle sorte que le public n'y ait pas accès.
 6. Le détenteur doit faire rapport au registraire de tout changement apporté aux renseignements qui paraissent sur la demande de permis, dans les 10 jours qui suivent cette modification; le détenteur doit en outre faire part des renseignements que le registraire peut lui demander de temps à autre.
 7. À la demande d'un agent de la paix, le détenteur doit montrer son permis de même que la permission d'achat des dispositifs d'interception qu'il a en sa possession ou qu'il est en train de fabriquer.
 8. Si un répondant retire son appui, le registraire révoquera ledit permis et transmettra une note à cet effet au détenteur.
 9. Le registraire peut révoquer un permis si le détenteur n'observe pas les conditions prescrites.
 10. Sauf indications contraires du registraire et avec l'approbation de ce dernier, le permis se termine à la date d'expiration qui y figure si le détenteur ne formule pas sa demande de renouvellement au moins trente jours avant ladite date.
 11. La demande de renouvellement doit être accompagnée d'une nouvelle lettre du répondant.
 12. Conditions spéciales.

DATE

OTTAWA, ONTARIO

RE ➤ Application for Licence — Sec. 178.18
— Protection of Privacy Act —

In reply to your letter of

Date _____

I am enclosing an application form. The following information will assist you in determining if you are eligible to be licenced.

Section 178.18 of the Criminal Code forbids the possession (including if applicable to manufacture) and/or sale of devices **primarily useful** for surreptitious interception of private communications, with certain exceptions. The section reads as follows:

178.18 (1) Every one who possesses, sells or purchases any electromagnetic acoustic, mechanical or other device or any component thereof knowing that the design thereof renders it primarily useful for surreptitious interception of private communications is guilty of an indictable offence and liable to imprisonment for two years.

(2) Subsection (1) does not apply to

(a) a police officer or police constable in possession of a device or component described in subsection (1) in the course of his employment;
(b) a person in possession of such a device or component for the purpose of using it in an interception made or to be made in accordance with an authorization;

(c) an officer or servant of Her Majesty in right of Canada or a member of the Canadian Forces in possession of such a device or component in the course of his duties as such an officer, servant, or member, as the case may be; and

(d) any other person in possession of such a device or component under the authority of a licence issued by the Solicitor General of Canada.

A copy of the usual terms and conditions which will be prescribed by the Solicitor General of Canada is attached. Unless special circumstances exist, a licence will only be granted to companies or individuals to provide sources of supply to police departments, the Canadian Forces, or the Canadian government.

Providing you have a sponsor (as defined in the terms and conditions) you may fill out the application and forward it to me with his letter of endorsement. A separate letter of endorsement is required from **each** sponsor with whom you intend to do business, i.e., if you intend to deal with three separate police departments you must be endorsed by all three. More than one letter of endorsement may accompany your application.

Should your application be successful a separate licence will be issued to you for each sponsor, permitting you to possess (including if applicable to manufacture) and/or sell devices in accordance with the specific authorization of the sponsor.

OBJET ➤ Demande de permis — Art. 178.18
— Loi sur la protection de la vie privée —

Pour faire suite à votre lettre du

je vous fais parvenir, sous pli, une formule de demande. Les renseignements qui suivent vous aideront à déterminer si vous pouvez obtenir un permis.

L'article 178.18 du Code criminel interdit la possession (la fabrication, s'il y a lieu) et la vente de dispositifs dont la conception les rend principalement utiles à l'interception clandestine de communications privées; il y a néanmoins certaines exceptions. L'article se lit ainsi:

178.18 (1) Est coupable d'un acte criminel et passible d'un emprisonnement de deux ans, quiconque possède, vend ou achète un dispositif électromagnétique, acoustique, mécanique ou autre ou un élément ou une pièce de celui-ci, sachant que leur conception les rend principalement utiles à l'interception clandestine de communications privées.

(2) Le paragraphe (1) ne s'applique pas

*(a) à un officier de police ou à un agent de police en possession d'un dispositif, d'un élément ou d'une pièce visés au paragraphe (1) dans l'exercice de ses fonctions;
(b) à une personne en possession d'un dispositif, d'un élément ou d'une pièce visés au paragraphe (1) qu'elle a l'intention d'utiliser lors d'une interception qui est faite ou doit être faite en conformité d'une autorisation;*

(c) à un fonctionnaire ou préposé de Sa Majesté du chef du Canada ou à un membre des Forces canadiennes en possession d'un dispositif, d'un élément ou d'une pièce visés au paragraphe (1) dans l'exercice de ses fonctions en tant que fonctionnaire, préposé ou membre, selon le cas; et

(d) à toute autre personne en possession d'un dispositif, d'un élément ou d'une pièce visés au paragraphe (1) en vertu d'un permis délivré par le solliciteur général du Canada.

Vous trouverez également ci-joint une copie des conditions prescrites par le Solliciteur général. À moins de cas exceptionnels, un permis ne sera accordé qu'à des compagnies ou à des particuliers pour assurer des fournisseurs aux services de police, aux Forces armées canadiennes ou au gouvernement du Canada.

*Si vous avez un répondant (tel que défini dans les Conditions), vous pouvez remplir une demande et me la faire parvenir accompagnée de la lettre du répondant. Il faudra fournir une lettre à part pour **chacun** des répondants avec lesquels vous entendez établir des relations d'affaires; en effet, si vous désirez traiter avec trois services de police, vous devez recevoir l'appui des trois. Votre demande peut être accompagnée de plus d'une lettre de répondant.*

Si votre demande est acceptée, un permis séparé à l'égard de chaque répondant vous sera délivré; il vous autorisera à posséder (à fabriquer s'il y a lieu) et à vendre des dispositifs en conformité de l'autorisation expresse du répondant.



REGISTRAR — LE RÉGISTRAR

NOTE

THIS LETTER MUST BE SIGNED BY THE CHIEF OF POLICE OF AN ACCREDITED POLICE FORCE, THE DIRECTOR OF CRIMINAL INVESTIGATION, THE DIRECTOR GENERAL SECURITY SERVICE, OR COMMANDING OFFICERS OF ANY DIVISION OF THE ROYAL CANADIAN MOUNTED POLICE, THE COMMISSIONER OF THE ONTARIO PROVINCIAL POLICE, THE DIRECTOR GENERAL OF THE QUEBEC POLICE FORCE, THE DIRECTOR GENERAL INTELLIGENCE AND SECURITY OF THE CANADIAN FORCES AND IN THE CASE OF AN OFFICER OR SERVANT OF HER MAJESTY IN RIGHT OF CANADA, THE HEAD OF THE BRANCH OF GOVERNMENT THAT EMPLOYS HIM OR OF WHICH HE IS AN OFFICIAL.

NOTE

CETTE LETTRE DOIT PORTER LES SIGNATURES DU CHEF D'UN SERVICE DE POLICE RECONNU, DU DIRECTEUR DE LA SÛRETÉ, DU DIRECTEUR GÉNÉRAL DU SERVICE DE SÉCURITÉ OU DES COMMANDANTS DIVISIONNAIRES DE TOUTE DIVISION DE LA GENDARMERIE ROYALE DU CANADA, DU COMMISSAIRE DE LA SÛRETÉ DE L'ONTARIO, DU DIRECTEUR GÉNÉRAL DE LA SÛRETÉ DU QUÉBEC, DU DIRECTEUR GÉNÉRAL DES RENSEIGNEMENTS ET DE LA SÉCURITÉ DES FORCES ARMÉES ET, DANS LE CAS D'UN FONCTIONNAIRE OU PRÉPOSÉ DE SA MAJESTÉ DU CHEF DU CANADA, DU CHEF DE LA DIRECTION DU GOUVERNEMENT QUI L'EMPLOIE OU DONT IL EST UN FONCTIONNAIRE.

LETTER OF ENDORSEMENT

THE REGISTRAR
LICENSING UNDER PROTECTION OF PRIVACY ACT

LETTRE DU RÉPONDANT

LE RÉGISTRARE
PERMIS DÉLIVRÉ AUX TERMES DE LA LOI SUR LA
PROTECTION DE LA VIE PRIVÉE

RE
OBJET

THIS IS TO CERTIFY I AM IN LAWFUL AUTHORITY OVER PERSONS WHO MAY POSSESS DEVICES PRIMARILY USEFUL FOR SURREPTITIOUS INTERCEPTION OF PRIVATE COMMUNICATIONS, PERMITTED BY SECTION 178.18 (2) (a) AND (c) OF THE CRIMINAL CODE.

I AM REQUESTING A LICENCE BE GRANTED TO

NAME
NOM

TO POSSESS, (INCLUDING, IF APPLICABLE, TO MANUFACTURE) AND/OR SELL THESE DEVICES ON MY BEHALF WHEN PROPERLY AUTHORIZED BY MYSELF.

I UNDERSTAND THAT PURSUANT TO SECTION 178.18 1 (d) THE DECISION WHETHER OR NOT TO ISSUE A LICENCE IS NOT SUBJECT TO APPEAL.

JE CERTIFIE PAR LES PRÉSENTES, AVOIR CHARGÉ LÉGALE DES PERSONNES AUTORISÉES À AVOIR DES DISPOSITIFS DONT LA CONCEPTION LES REND PRINCIPALEMENT UTILES À L'INTERCEPTION CLANDESTINE DE COMMUNICATIONS PRIVÉES, COMME LE PRÉVOIENT LES ALINÉAS 178.18 (2) a) ET c) DU CODE CRIMINEL.

JE DEMANDE À CE QUE L'ON DÉLIVRE UN PERMIS À

EN VUE DE LA POSSESSION (DE LA FABRICATION, S'IL Y A LIEU) ET DE LA VENTE DE DISPOSITIFS EN MON NOM LORSQUE JE L'Y AUTORISE.

JE CROIS SAVOIR QUE, SUIVANT L'ALINÉA 178.18 (1) d), LA DÉCISION D'ACCORDER OU DE REFUSER UN PERMIS EST SANS APPEL.

SIGNATURE

May 22, 1975

**X WATERGATE REORGANIZATION
AND REFORM ACT—S. 495**

AMENDMENT NO. 495

(Ordered to be printed and referred to the Committee on Government Operations.)

Mr. PERCY. Mr. President, with the cosponsorship of Senator BAKER and after a year's staff research and study, I am today submitting an amendment to S. 495, the Watergate Reorganization and Reform Act.

Many of the crimes and abuses which fell beneath the umbrella label of "Watergate" were associated with the practice of electronic eavesdropping and wiretapping. The tapping of newsmen and executive employees by the "White House Plumbers," the clandestine tape recording of White House conversations both in the Oval Office and over White House telephones, as well as the actual attempted bugging of the Democratic National Headquarters at the Watergate Hotel complex, are all prime examples of the sorts of invasions of privacy now rendered frighteningly simple by modern technology. In this sense, the Watergate scandals and so-called "White House horrors" were symptomatic of something more than the simple abuse of power. Rather, they must be viewed as part of a larger question facing American society today, that of technology run rampant.

It is the intent of the Watergate reform bill to establish effective preventive measures to help insure that this Nation is not subjected to more than one Watergate. This amendment would further effectuate that goal by dealing with the problem of electronic eavesdropping and wiretapping which was at the very heart of the Watergate scandals.

The amendment that I am submitting today attempts to deal with the problem of clandestine electronic snooping. The approach is essentially threefold: First, regulation of the manufacture, distribution, and possession of the devices themselves; second, tightening of the applicable law so as to require notice to or consent of all parties to a conversation before it may legally be electronically or mechanically overhead or recorded, except in those cases where a judicial warrant has been obtained; and third, facilitation of the civil remedy in cases of illegal eavesdropping by insuring access by the potential plaintiff to the investigatory resources of law enforcement and the telephone companies. By thus limiting the availability of electronic eavesdropping devices and further defining the rights of the victims of their abuse, it is my hope that this amendment will significantly lessen the now prevalent fear that no conversation is ever truly private.

Titles V through VII of the amendment create a regulatory system requiring the obtaining of a license in order to manufacture, import, sell, transfer, or possess an electrical or mechanical eavesdropping device. An eavesdropping "device," for the purpose of this section, is one of a narrowly defined type of device which can by its nature be used to intercept a wire or oral communication without the knowledge of all parties, and, in addition, is not primarily or ordinarily used for anything else. Section 201(3). Only those products which are created for the sole and primary purpose of surreptitious eavesdropping would fall under the purview of regulation. Thus while a simple everyday tape recorder would not fall under the definition, a disguised tinfo microphone specially designed to be able to pick up a conversation while in hiding would most certainly be subject to regulation.

The purpose of the regulation system is then a two-fold one of limiting the distribution of eavesdropping devices only to those who have a justifiable legal purpose for having them, and at the same time of creating a systematic means for keeping track of the device discovered in the course of an investigation, as well as that of its rightful owner.

The information gathering system will operate on a simple "chain of title" basis. Every device produced, manufactured, or imported must be in effect baptised for life with a nonerasable identification number. This number will then be placed on the head of a file. Any further sales, transfers, or other dispositions of the device will then be recorded in this same file.

At present, one of the single greatest roadblocks to effective enforcement of the wiretap laws is the inability of investigators to trace back a device which they have found to its actual owner. Under my legislation, if an investigator does in fact come up with such a device, it will be but a simple matter to check the number on the device, look up the file under that number, and discover the name of the manufacturer, the record of all sales and transfers of the device, and the name of its most recent owner.

For the purpose of limiting the actual distribution of the devices, of keeping them in the hands of responsible individuals with valid purposes for their use, two types of licenses will be issued by the Secretary of Commerce under the regulatory scheme; "business licenses" for those who wish to engage in the manufacture, assembly, importation, transfer, or sale of the devices, and "possessor licenses" for those who wish to own, possess, or actually use such devices. Both licenses will be limited to those

who, upon application, can state a valid and lawful purpose for their particular dealings in eavesdropping devices. For the business license, the applicant must state fully his present and foreseeable activities in the area. For the possessor license, the applicant must state just what he intends to do with the device once it is in his hands. In addition, if after a hearing it is found that either applicant has been convicted of, or is likely to be engaged in, an eavesdropping-related offense, the Secretary will deny the license application.

Through this regulatory mechanism we will hopefully be able to separate responsible use from irresponsible, legitimate use from illegitimate, and based upon this knowledge, be able to limit the right to own or use such devices.

One example where such a system has been successfully put into practice is that of the State of Maryland. Maryland law requires manufacturers and possessors of eavesdropping equipment to register their devices. It further requires reports on all sales and transfers of such devices. Thus far, 71 devices have been registered to 10 persons and corporations. Though on a smaller scale, certainly the success of the Maryland experiment in this field demonstrates the feasibility and advantageousness of the system I propose today. In discussing his experience with the operation of the Maryland system, Superintendent Smith of the Maryland State Police concluded:

I would definitely favor the establishment of laws providing for the licensing of such (eavesdropping) equipment. . . . I would also favor the licensing of manufacturers of such devices.

Mr. President, title IX of my amendment tightens the Federal wiretap law by eliminating some of its more crippling weaknesses. The present state of the law with regard to eavesdropping and electronic bugging is just about as solid as a doughnut. The big gaping hole in the center to which I draw your specific attention is the "one party consent" exception. That is, the law specifically forbids the practice of warrantless interception of wire and oral communications unless one of the parties to the conversation has given his consent. This single party consent, so the law goes, can indeed be the eavesdropper himself. Such being the case, the rights of the other parties to a conversation against such eavesdropping are rendered a nullity.

The potentiality for abuse under this law is immense. Take, for example, the case of a Mr. Smith, who, after confiding to a friend one night over the telephone, woke up the next morning to find a verbatim transcript of the juicier parts of his conversation in the morning newspaper. His supposed friend, it seems, had taken the trouble of recording the entire conversation, without providing our Mr. Smith with any forewarning as to his actions or intentions. When Mr. Smith

then sued his former friend and the newspaper, he lost. Because the conversation had been recorded by one of its participants, the tap was deemed perfectly legal under the one-party consent exception. Unfortunately, this was an actual case. *Smith v. Cincinnati Post and Times Star*, 353 F. Supp. 1126.

A more recent example of abuse under this exception to the law is seen in the famous White House tapes. While outrageous on its face, it was in fact perfectly legal for the former President to secretly tape record conversations in his Oval Office as well as over his telephones without warning or notice to other unaware parties to such conversations. The former President himself, in this case, was the single-party consent. The fact that he knew about the presence of the taping system was in itself enough to guarantee legality as long as he was present, despite the fact that those whose words he recorded had no knowledge of the recording, nor had consented to it.

Title IX of my amendment puts a plug in the doughnut hole by amending the present 18 United States Code, section 2511 to require "the consent of all parties" to an interception committed without a judicial warrant of any wire or oral communication. This provision would provide assurance that no private conversation can be electronically or mechanically overheard or taped without either the consent of all parties to the conversation, or a judicial warrant authorizing such overhearing or taping.

It is not the intent of this provision to interfere with the ability of the police to conduct their investigations into alleged wrongdoing by means of electronic surveillance. Title 18 lays out in much detail a fair and effective mechanism for law enforcement officials to obtain warrants for such surveillance when the requisite probable cause and other criteria exist. It is the intention of this provision to prevent law enforcement from bypassing or circumventing the statutory safeguards through the use of the one-party consent exception, that is, to make the tapped telephone calls themselves, or via a collaborator, record the conversation, and then use the recording as court admissible evidence, all without the use of a warrant, without probable cause—all technically legal now. At present, a law enforcement official recording such a conversation would be a party to the conversation and, therefore, could consent to its interception. See *Commonwealth v. Murray*, 423 Pa. 37.

As a further attempt to tighten the reins against abuse of the wiretap and eavesdrop laws, my amendment sets forth specific sanctions against those who knowingly break the rules. The recent case of *United States v. Giordano*, 416 U.S. 505 (1974), which involved forged signatures of the Attorney General's name upon previously prepared surveillance authorizations, flying directly in

the face of a statutory requirement, is a case in point. The exclusionary rule, no matter how diligently applied by the courts, is simply ill-equipped to deal with such high level chicanery. Only a direct sanction against the offending officer himself can fulfill this function. This is what my amendment attempts to do.

As an attempt to facilitate the ability of private individuals to bring their own civil actions in the event that they themselves are subject to an illegal eavesdrop, two specific steps are taken. First, as a means of lightening the burden of proof, a standard is set by which any conviction of a defendant in a criminal proceeding brought against him on a charge concerning a violation of the wiretap laws will be regarded as conclusive in a civil proceeding brought against him regarding the same violation. Through this manner, the civil litigant will be able to benefit from the investigative and organizational resources of law enforcement, to ride on the prosecutor's coattails, so to speak. Second, an affirmative duty is placed on the telephone companies to aid their customers in investigating such offenses. Many of these companies do at the present follow a policy similar to that set down in my amendment. Some others, however, do not. The intention of this provision of my amendment is to make the practice uniform and mandatory.

This legislation would affect the phone company in a number of other ways as well. At present, there is no duty for a phone company to report a tap to the police which it has discovered on a customer's line. Although almost all phone companies do report such taps at present, an exception is Illinois Bell Telephone. This legislation would require phone companies to report the discovery of a tap to a law enforcement official.

In addition, phone companies are now allowed to secretly tape conversation when they believe that a fraud is being committed against the phone company. They do not have to prove probable cause; they do not have to get anyone's permission; they have a free hand in deciding whether a crime is being committed and whether a conversation should be recorded. This unbridled discretion is unparalleled. No other industry or private citizen has such discretion, and even the police have to obtain a court order before secretly recording conversations. This legislation would remove this discretion from the phone companies and make them seek the help of the police and the approval of a court if they suspect a crime is being committed. The police may seek a court order to intercept a conversation if the conditions for such a court order can be met. This will not hinder the phone companies since their technology is such that they can pretty well determine when a fraud is being committed, and thereby prove probable cause to a court.

But, no longer would they be free to tape conversations whenever in their discretion they felt it was warranted.

The issues with which the amendment deals are important to us both as legislators and as individuals. As legislators, we must attempt to deal with a social problem which has of its own momentum played a large role in one of the greatest national catastrophes of our day. As individuals, we have at stake the quality of the environment in which we work, act, think, and communicate every day of our lives. Both of these responsibilities are weighty.

Mr. President, I ask unanimous consent that a statement by Senator BAKER be printed in the RECORD and that the amendment be printed in the RECORD.

There being no objection, the statement and amendment were ordered to be printed in the RECORD, as follows:

STATEMENT BY SENATOR BAKER

I welcome the opportunity to join my distinguished colleague from Illinois (Mr. PERCY) in introducing this amendment to S. 496, the "Watergate Reorganization and Reform Act."

As I noted in my individual views for the Final Report of the Select Committee on Presidential Campaign Activities, "I believe that Congress should carefully consider a prohibition of the electronic recording of conversations . . . except with the prior consent of all the participants to the conversation, or unless carefully supervised by a court of competent jurisdiction for specified statutory purposes." I believe that S. 459, the Watergate Reorganization and Reform Act, provides a timely and appropriate vehicle for the Congress to consider such a prohibition of non-consensual electronic eavesdropping and wiretapping occurring without prior judicial approval; and I commend Senator Percy for his leadership in this area.

Certainly the single most notable evidentiary achievement of the Senate Watergate Committee was the revelation by Alexander Butterfield of the tape recording system utilized in both the Oval Office and the Presidential Suite in the Executive Office Building. I am not sure that I understand why the tape-recording facilities were installed; but I find the practice of recording conversations without the consent of all parties thereto, in the absence of a warrant, objectionable and not in keeping with the grandeur of the Fourth Amendment.

I further believe that this amendment is reflective of the sentiment of what I consider to be one of the most important recommendations of the Senate Watergate Committee. That is, the Select Committee on Presidential Campaign Activities in its Final Report recommended "that the appropriate committees of Congress study and reconsider Title III of the Omnibus Crime and Safe Streets Act of 1968 for the purpose of determining whether the electronic surveillance provisions contained in that Act require revision or amendment." In *United States v. U.S. District Court*, 407 U.S. 297 (1972), the Supreme Court pointedly invited Congress to decide whether prior judicial approval is required for all law-enforcement and intelligence surveillance; and the Watergate Committee so recommended. I recognize that legitimate law-enforcement and intelligence requirements often mandate such surveillance; but, in my opinion, when it is

done within the United States, it is preferable that a warrant be obtained prior to implementation.

This amendment, of course, also would require regulation of electronic eavesdropping devices and makes clear civil remedies in cases of illegal eavesdropping. If we allow the manufacture and distribution of eavesdropping devices and wiretaps to continue unchecked, we may find that there may come a time at which no conversation, however private or personal, will be secure from the curious or the rampant opportunist.

I believe that the amendment which Senator Percy and I are introducing today reflects a serious attempt to eliminate what I consider to be perhaps the most objectionable abuse uncovered by the Select Committee on Presidential Campaign Activities, and I think that it reflects the concern underlying one of the major recommendations of the Senate Watergate Committee. It certainly is pertinent to the Watergate-prompted reform effort, and I commend it to my colleagues.

AMENDMENT No. 496

On page 37, line 15, add the following:
TITLE V—LICENSING OF ELECTRONIC,
MECHANICAL, OR OTHER DEVICE

SEC. 501. As used in this title, the term—

(1) "business license" means a certificate, paper, or other item issued by the Secretary to any applicant in the business of manufacturing, importing, assembling, transferring, or selling of electronic, mechanical, or other devices;

(2) "possessor license" means a certificate, paper, or other item issued by the Secretary to any applicant owning, possessing, or otherwise having in his custody any electronic, mechanical, or other device;

(3) "electronic, mechanical, or other device" shall have the same meaning as that provided for under section 2510(5) of title 18, United States Code, except that, for purposes of this Act, the Secretary shall issue regulations excluding from such term any electronic, mechanical, or other device which the Secretary determines, on the basis of the design, size, and nature thereof, is primarily and ordinarily used for a purpose other than the overhearing of oral communications of others without their knowledge;

(4) "Secretary" means the Secretary of Commerce; and

(5) "person" means any individual, association, partnership, institution, corporation, or other entity, any officer, employee, or agent of the United States or any territory or possession thereof, or of any State or political subdivision thereof.

SEC. 502. (a) On and after the expiration of the one hundred and twentieth day following the date of the enactment of this Act, no person shall engage in the business of manufacturing, assembling, importing, transferring, or selling of any electronic, mechanical, or other device, if such device or component thereof has been or will be sent through the mail or transported in interstate or foreign commerce, unless such person has a valid business license issued to him in accordance with this title.

(b) The Secretary is authorized, upon application to him by an applicant in accordance with this title, to issue to such applicant a business license, unless the Secretary determines, after a hearing, that such applicant has been convicted of a violation of chapter 119 of title 18, United States Code, that there is a substantial probability that

such applicant is engaged, or is likely to engage, in conduct in violation of chapter 119 of title 18, United States Code, or that such applicant has knowingly submitted false or misleading information in connection with his application for such license, or in connection with any other application, document, notice, or paper submitted pursuant to this Act.

(c) Any business license issued pursuant to this title may, after a hearing, be revoked or otherwise suspended by the Secretary if he determines that the holder of such license has been convicted of a violation of chapter 119 of title 18, United States Code, or has knowingly submitted false or misleading information in connection with his application for such license, or in connection with any other application document, notice, or paper submitted pursuant to this Act.

(d) Applications under this section shall be submitted to the Secretary on such form as the Secretary shall provide. Any such application shall contain, among other matters, the following:

(1) name and address of the applicant;

(2) business or trade name of the applicant;

(3) a complete description of the applicant's business or dealings insofar as such business or dealings involve electronic, mechanical, or other devices;

(4) the address of each location where the applicant conducts or will conduct business or other dealings involving electronic, mechanical, or other devices; and

(5) any other information or data which the Secretary may, by regulation, prescribe.

(e) Any business license issued pursuant to this section shall, unless revoked or suspended in accordance with this title, be valid for a period of twelve months. Each such license issued under this section shall be identified by a reference number issued by the Secretary. Any person holding a valid business license issued under this section shall notify the Secretary, in writing, of any changes in the information provided on the application for such license. Such notice shall be submitted prior to the expiration of the fourteen day period following such change.

(f) Any person violating the provisions of subsection (a) of this section shall be fined not more than \$10,000 or imprisoned not more than five years, or both.

SEC. 503. (a) On and after the expiration of the one hundred and fiftieth day following the date of the enactment of this Act, no person, other than a person having a valid business license issued to him under this title, shall own, possess, or otherwise have in his custody, any electronic, mechanical, or other device, if such device or component thereof has been or will be sent through the mail or transported in interstate or foreign commerce, unless such person has a valid possessor license issued to him in accordance with this section.

(b) The Secretary is authorized, upon application to him by an applicant in accordance with this section, to issue to such applicant a possessor license, unless the Secretary determines, after a hearing, that such applicant has been convicted of a violation of chapter 119 of title 18, United States Code, that there is a substantial probability that the ownership, possession, or custody by such applicant of any electronic, mechanical, or other device would be unlawful under the provisions of section 2512 of title

18, United States Code, that there is a substantial probability that such applicant is engaged, or is likely to engage, in conduct in violation of chapter 119 of title 18, United States Code, or that such applicant has knowingly submitted false or misleading information in connection with his application for such license, or in connection with any other application, document, notice, or paper submitted pursuant to this Act.

(c) Any possessor license issued pursuant to this section may, after a hearing, be revoked or otherwise suspended by the Secretary if he determines that the holder of such license has been convicted of a violation of chapter 119 of title 18, United States Code, or has knowingly submitted false or misleading information in connection with his application for such license, or in connection with any other application, document, notice, or paper submitted pursuant to this Act.

(d) Applications under this section shall be submitted to the Secretary on such form as the Secretary shall provide. Any such application shall contain, among other matters, the following:

- (1) name and address of the applicant;
- (2) business or trade name, if any, of the applicant;
- (3) a complete description of the applicant's business or dealings, if any, insofar as such business or dealings involve electronic, mechanical, or other devices;
- (4) the address of each location, if any, where the applicant conducts or will conduct business or other dealings involving electronic, mechanical, or other devices;
- (5) a statement of the purpose to which the applicant intends to put the electronic, mechanical, or other device for which application is made;
- (6) a statement as to whether the applicant has been denied a business license or possessor license under this title, or had any such license suspended or revoked;
- (7) the number, description, and identification number of all electronic, mechanical, or other devices owned or possessed by the applicant, or in his custody at the time of such application and during the twelve month period preceding the date of such application, except that the requirement as to identification number shall not be applicable, with respect to any such device so owned, possessed or in the custody of any such applicant for any period prior to the date of expiration of the one hundred and twenty day period following the date of the enactment of this Act; and
- (8) any other information or data which the Secretary may, by regulation, prescribe.

(e) Any possessor license issued pursuant to this section shall, unless revoked or suspended in accordance with this title, be valid for a period of twelve months. Each such license issued under this section shall be identified by a reference number issued by the Secretary. Any person holding a valid possessor license issued under this section shall notify the Secretary, in writing, of any material change in the information provided on the application for such license. Such notice shall be submitted prior to the expiration of the fourteen day period following such change.

(f) In addition to information required under subsection (d) of this section, any law enforcement officer applying for a possessor license under this section shall submit to the Secretary the following:

- (1) law enforcement agency by which the applicant is employed;

(2) the name and address of his commanding officer;

(3) If the applicant is a Federal law enforcement officer, such application shall contain assurances by the Attorney General or his designee to the effect that the applicant is of good standing and good character and whose assigned duties may involve the use of electronic, mechanical, or other devices;

(4) If the applicant is a State or local law enforcement officer, such application shall contain assurances by the chief law enforcement officer of the State or his designee to the effect that the applicant is of good standing and good character and whose assigned duties may involve the use of electronic, mechanical, or other devices.

(g) In the event that a law enforcement officer holding a valid possessor license ceases to be a law enforcement officer, such license shall be deemed revoked and of no force and effect, and the commanding officer of such law enforcement officer shall so notify the Secretary to that effect.

(h) Any person violating the provisions of subsection (a) of this section shall be fined not more than \$10,000 or imprisoned not more than five years, or both.

TITLE VI—IDENTIFICATION; REGISTRATION

Sec. 601. (a) On and after the expiration of the one hundred and twentieth day following the date of the enactment of this Act, no person engaged in the business of manufacturing, importing, or assembling electronic, mechanical, or other devices for which a license is required under this Act shall sell, transfer, distribute, or otherwise dispose of any such device so manufactured, imported, or assembled unless such device shall have affixed to it in such a manner that it cannot be readily removed, altered or obliterated, an identification number issued by the Secretary in accordance with this title.

(b) On and after the expiration of the one hundred and fiftieth day following the date of the enactment of this Act, no person shall own, possess, or otherwise have in his custody, transfer, or sell, any electronic, mechanical or other device unless such electronic, mechanical, or other device has affixed to it in such a manner that it cannot be readily removed, altered, or obliterated an identification number issued by the Secretary in accordance with this title.

(c) Upon approval by him of any application received from any person engaged in the business of manufacturing, assembling, importing, selling, or otherwise distributing electronic, mechanical, or other devices, or from any person owning, possessing, or otherwise having custody of any electronic, mechanical, or other device, for an identification number for purposes of this title, the Secretary is authorized to issue such number if he determines that such application contains such information as is required by, and is in compliance with, regulations issued by him for purposes of this title.

(d) Any person who sells, transfers, distributes, or disposes of any electronic, mechanical, or other device in violation of subsection (a) of this section or any person who owns, possesses, or otherwise has in his custody any electronic, mechanical, or other device in violation of subsection (b) of this section, shall be fined not more than \$10,000 or imprisoned not more than five years, or both.

Sec. 602. (a) The Secretary is authorized and directed to establish and carry out, and

Keep current, a program of registration of all electronic, mechanical, or other devices in the United States. Such program shall be established and carried out with a view to requiring each person (other than a person covered by subsection (b)), within sixty days following the date he acquires ownership, possession, or other custody of any electronic, mechanical, or other device, or within the one hundred and fifty day period following the date of the enactment of this Act, whichever last occurs, to register such electronic, mechanical, or other device with the Secretary.

(b) On and after the expiration of the one hundred and fiftieth day following the date of the enactment of this Act, no person engaged in the business of manufacturing, importing, or assembling of any electronic, mechanical, or other device for which a license is required under this Act shall sell, transfer, distribute, or otherwise dispose of any such device unless such device has been registered in accordance with subsection (a) of this section.

(c) Such registration shall be carried out on forms made available by the Secretary and containing, among other matters, the following:

(1) the identification number of the device;

(2) the name (including business or trade name, if any), address (including business address, if any) and number of the business license or the possessor license of the person so registering such device; and

(3) a complete description of the electronic, mechanical, or other device to be so registered.

(d) Any person who violates the provisions of subsection (a) or (b) of this section shall be fined not more than \$10,000 or imprisoned not more than five years, or both.

TITLE VII—SALE OR TRANSFER OF ELECTRONIC, MECHANICAL, OR OTHER DEVICE

SEC. 701. (a) On and after the expiration of the one hundred and fiftieth day following the date of the enactment of this Act, no person engaged in the business of manufacturing, importing, or assembling of any electronic, mechanical, or other device for which a license is required by this Act, and no person owning, possessing, or otherwise having in his custody, any electronic, mechanical, or other device for which a license is required under this Act, shall sell, transfer, distribute, or otherwise dispose of any electronic, mechanical, or other device, unless any such person has, not less than fourteen days prior thereto, notified the Secretary, in writing, concerning such intended sale, transfer, distribution, or other disposition. Such notice shall include, among other matters, the following:

(1) the name, address, and number of the business or possessor license issued under this Act of the person so selling, transferring, distributing, or otherwise disposing of such device;

(2) the name, address, and number of the business or possessor license issued under this Act of the person to whom such device is to be so sold, transferred, distributed or disposed of;

(3) the identification number of such device, obtained pursuant to this Act;

(4) a statement of the purposes for which such device is to be so used; and

(5) any other information which the Secretary may, by regulation, require.

(b) The Secretary may, within the fourteen day period following the receipt by him of any such notice of intention to sell, transfer, distribute, or otherwise dispose of any electronic, mechanical, or other device, issue an order prohibiting the carrying out of such intended sale, transfer, distribution, or disposition covered by such notice, if the Secretary determines that—

(1) the person to whom such electronic, mechanical, or other device is to be sold, transferred, distributed, or disposed of does not have a valid business license or possessor license issued pursuant to this Act;

(2) new information concerning such person referred to in paragraph (1) would be grounds for suspending, revoking, or not renewing any valid business license or possessor license held by such person;

(3) information in any such notice under subsection (a) of this section is false or incomplete;

(4) there is a substantial probability that such device to be so sold, transferred, distributed, or disposed of will be used for an unlawful purpose.

(c) In any case in which no order is issued pursuant to subsection (b) of this section with respect to any notice, the person submitting such notice shall, following the expiration of the fourteen day period following the submission of such notice, be authorized to carry out such sale, transfer, distribution or disposition covered by such notice.

(d) Any person who sells, transfers, distributes, or disposes of any electronic, mechanical, or other device in violation of the provisions of subsection (a) of this section, or in violation of any order pursuant to subsection (b) of this section, shall be fined not more than \$10,000 or imprisoned not more than five years, or both.

TITLE VIII—DUTIES OF THE SECRETARY; AUTHORIZATIONS

SEC. 801. The Secretary shall take such action as may be necessary to assure that all information or other data obtained by him in connection with the issuance of business licenses, possessor licenses, the sale, transfer, distribution, or other disposition of electronic, mechanical, or other devices, including the identification numbers thereof and the registration with respect thereto, is kept in a central place and in such a manner as to facilitate the retrieval or abstraction of the aforementioned information and data, except that all information and data concerning the issuance of a possessor license to a law enforcement officer may be kept confidential if requested by the commanding officer of the applicant. In any case involving such a request, such information or data may be made available to any appropriate court or law enforcement agency upon receipt of a proper request or order, but shall be so made available under such condition or conditions as the Secretary may impose to assure the confidentiality of such information and data.

SEC. 802. As soon as practicable following the date of the enactment of this Act, but in no event later than sixty days following such date, the Secretary shall issue such regulations as may be necessary to carry out the provisions of this Act.

SEC. 803. The Secretary shall, on not less than an annual basis, report to the Congress concerning the administration and operation of this Act. Such report shall include, among other matters—

(1) the number of applications for business and possessor licenses received by the Secretary during the calendar year preceding

the calendar year in which such report is submitted;

(2) the number of such licenses issued during such period covered by such report;

(3) the number of possessor licenses issued to law enforcement officers during such period covered by such report;

(4) the number of electronic, mechanical, or other devices manufactured, assembled, or imported to the United States, and the number of sales, transfers, distributions, or other dispositions thereof during such period;

(5) the estimated number of electronic, mechanical, or other devices in the United States during such period; and

(6) such other information or data as the Secretary may, by regulation, require.

Sec. 804. There are authorized to be appropriated such sums as may be necessary to carry out the provisions of this Act.

TITLE IX—ALL PARTY CONSENT

Sec. 901. (a) Paragraph (a) of section 2511(1) of Title 18, United States Code, is amended by inserting immediately before the semicolon at the end thereof a comma and the following: "without the consent of all the parties to such communication."

(b) Paragraph (b) of section 2511(1) of Title 18, United States Code, is amended by inserting immediately after the word "communication" a comma and the following: "without the consent of all the parties to such communication."

(c) Section 2511(1) of chapter 119 of Title 18, United States Code, is amended by inserting immediately after paragraph (d) the following new paragraph:

"(e) willfully fails to report to a law enforcement official within a reasonable time any violation of this chapter;"

(d) Section 2510(4) of chapter 119 of Title 18, United States Code, is amended by deleting the period and inserting after the word "device" the following: "in any manner which allows someone not a party to such communication to hear or record the contents of such communication."

Sec. 902. Section 2511(2) of chapter 119 of Title 18, United States Code, is amended by striking out paragraphs (c) and (d) and inserting in lieu thereof the following:

"(c) It shall not be unlawful under this chapter for any person to intercept and record conversation over his own telephone or upon his own premises and to which he is a party, if—

"(1) notice is given to all other parties to such conversation that the conversation is being intercepted or recorded, or both; and

"(2) the contents of any such interception or recording is not divulged to any person not a party to such conversation without the consent of all other parties to the conversation.

"(d) It shall not be unlawful under this chapter to record or otherwise tape any conversation in a public place which is otherwise readily audible without the use of any electronic, mechanical, or other device, and which takes place under circumstances such as not to afford a reasonable expectation of privacy, if such conversation is not recorded or taped for purposes either tortious or criminal."

Sec. 903. Section 2520 of Title 18, United States Code, is amended by adding at the end thereof the following new sentence: "Any criminal conviction obtained under this chapter shall be conclusive in any such civil action."

Sec. 904. (a) Chapter 119 of Title 18, United States Code, is amended by adding at the end thereof the following new section:

"Sec. 2521. SANCTIONS

"(a) (1) Any person who willfully violates the procedural provisions of this chapter;

"(2) Any existing officer who willfully exceeds the authority of his warrant;

"(3) Any person who willfully divulges any information obtained by lawful intercept under this chapter to any unauthorized person or agency; or

"(4) Any person who willfully violates any person's constitutional or statutory rights under this chapter shall be deemed in contempt of court and subject to a fine of \$10,000 or imprisoned for not more than five years, or both.

"(b) Any law enforcement officer who—

"(1) willfully violates any of the procedural provisions of this chapter;

"(2) willfully exceeds the authority of any warrant issued under this chapter in the course of executing such warrant; or

"(3) willfully violates the constitutional or statutory rights of any person under this chapter shall be fined not more than \$10,000 or imprisoned for not more than five years, or both."

(b) The section analysis of chapter 119 of title 18 of the United States Code is amended by adding at the end thereof the following new item:

"2521. Sanctions."

Sec. 905. The Communications Act of 1934, as amended, is amended by adding at the end of title II the following new section:

"Sec. 223. (a) Telephone and telegraph companies shall, upon the written request of a subscriber, furnish whatever service possible for the purpose of detecting any unlawful interception of communication carried on through the facilities of such common carrier. All such requests by subscribers shall be subject to the provisions of chapter 119 of title 18, United States Code.

"(b) It shall be the affirmative duty of every telephone and telegraph company or officer or employee thereof to report to a law enforcement agency immediately upon discovery of any violation of the provisions of such chapter 119 discovered in the course of normal operations in response to a request of a subscriber as provided in subsection (a) of this section, or in any other manner. It shall further be the duty of any such telephone or telegraph company or officer or employee thereof to make available to law enforcement personnel any information relevant to such reports or discoveries as are needed for prosecutions under chapter 119 of title 18, United States Code.

"(c) Every telephone and telegraph company shall keep records and make annual reports to the Secretary. Such reports shall include—

"(1) the number of requests pursuant to subsection (a) of this section that it receives from subscribers;

"(2) the number of times pursuant to such requests or by other independent action on the part of such telephone or telegraph company—

"(A) an electronic, mechanical, or other device (as defined in section 2510 (5) of Title 18, United States Code), or evidence thereof, was discovered,

"(B) any person was arrested for violation of chapter 119 of Title 18, United States Code, and the disposition of such cases,

"(C) a cataloging of the types of devices discovered;

"(D) the number of such electronic, mechanical, or other devices discovered, and

"(E) the cost incurred by the reporting company in carrying out the requirements of this section."

SEC. 906. (a) Section 2511 (2) (a) of Title 18, United States Code, is amended by striking the period at the end thereof and inserting the following:

"; *Provided further*, That no operator of a switch board, or an officer, employee, or agent of any communication common carrier, whose facilities are used in the transmission of wire communications, may intercept or mechanically or otherwise record any oral communication over such facilities for the purpose of protecting the rights or property of the carrier of such communication."

(b) Section 2516 (1) of Title 18, United States Code, is amended by redesignating subsection "(g)" as subsection "(h)", and adding a new subsection "(g)" as follows:

"(g) any offense involving fraud by wire under section 1843 of this Title."

CHAIRMAN ERICKSON: The first witness is Mr. Bower.

The questioning will commence by Mr. Michael Hershman of the staff.

MR. HERSHMAN: Mr. Bower, I understand you have an opening statement?

MR. BOWER: Yes.

MR. HERSHMAN: Please proceed.

**TESTIMONY OF A. T. BOWER,
MANAGER, GOVERNMENT SALES,
BELL & HOWELL COMMUNICATIONS
COMPANY: ACCOMPANIED BY DAVID
M. DORSEN, ESQ.**

MR. BOWER: Mr. Chairman and members of the Commission, thank you very much for the opportunity to appear before you.

I am Manager for Government Sales, of Bell & Howell Communications Company.

This is a division of Bell & Howell Company, a publicly-held corporation long a household word in the field of motion picture projectors.

The Communications Company had its origins in the Kel Corporation, which was formed about 1956 and which introduced the well-known Kel-Com 2-way transceiver.

The assets of the Kel Corporation were acquired by Bell & Howell in 1968 and a program of expansion was begun in the area of pocket-paging and, later and to a lesser degree, in electronic surveillance equipment.

Within the Bell & Howell Communications Company is a separate organization whose activities involve support of the domestic law enforcement community. This organization is known as the Special Operations Group.

Over the years the Special Operations Group has made its equipment, technical support, and operational experience available to law enforcement agencies at the federal, state and local levels.

I would like to direct my introductory remarks to some of the problems we, as a manufacturer of electronic surveillance equipment, encounter as a result of our attempts to comply with both the letter and the spirit of the Omnibus Crime Control and Safe Streets Act of 1968.

Before doing so, however, I would like to make three observations:

First, we recognize that the national policy concerning the use of electronic surveillance equipment is established by the government—the Congress, the Executive Branch, and the courts. Under the present law and policy the surreptitious interceptions of wire and oral communications by law enforcement agencies are permitted under carefully

defined circumstances and controls. The premise of the law and policy is that controlled surreptitious interception is important to the goals of legitimate law enforcement. So long as this is our national policy, Bell & Howell hopes to continue to make its contribution in this field.

Second, we will continue to do everything humanly possible to act within the letter and spirit of the law and encourage others to do so. For example, we make copies of the Omnibus Crime Control and Safe Streets Act of 1968 available to all our customers at no cost. Field sales representatives encourage a full awareness, on the part of law enforcement administrators, of the need to insure effective and legal performance from their operation intelligence sections. We point out that indiscriminate, inept or illegal use by intelligence officers of their sensitive equipment could help destroy the integrity and effectiveness of the total law enforcement effort.

Third, we at Bell and Howell are acutely conscious of the importance our society places on the individual's right to privacy. Our concern for this value is always present.

For example, because of the possibilities for abuse inherent in the tapping of telephones, Bell & Howell has made the decision to refrain from manufacturing equipment designed for this purpose even though the manufacture of telephone tapping equipment would be legal.

In the few minutes I have remaining, I would like to mention three of the problem areas in interpreting and complying with Section 2512 of Title 18 of the United States Code, which governs the manufacture of intercepting devices. We hope that among your recommendations will be suggestions to provide better guidelines to manufacturers who are trying to operate in full compliance with the law while fulfilling the needs of law enforcement.

First, the very definition of the devices covered by Section 2512 of Title III of the Act requires clarification.

Section 2512 applies to any device the design of which "renders it primarily useful for the purpose of the surreptitious interception of wire or oral communications." The phrase "primarily useful" has given us considerable difficulty. While perhaps it is undesirable—or impossible—to make the statute more specific, certain guidelines are necessary and no one, including the Department of Justice, has been willing to provide any assistance in this regard despite seven years of experience applying and enforcing the Act.

Second, Section 2512 permits the manufacture of surveillance devices by a person who is "under contract with" a bona fide law enforcement agency.

We at Bell & Howell have construed this provision to mean that we cannot manufacture a surveillance device until we have a contract with the purchaser. The impact of this provision is immense. There is a six-to-twelve-week lag from order to delivery with consequent impact on the law enforcement agency; the cost to the purchasing agency is higher because we must manufacture the devices to order; demonstration of our products to the purchasing agency is severely limited; and research and development are seriously hindered.

One possible solution to this problem is instituting a rigorous licensing inspection system. We at Bell & Howell urge the adoption of such a system as a more desirable alternative to the present law and pledge our full cooperation to its implementation and policing.

Third, Section 2512 permits the sale of surveillance devices pursuant to a contract with "the United States, a State, or a political subdivision thereof in the normal course of the activities" of the United States, the State or the political subdivision.

It has been suggested, I believe, that when a manufacturer, pursuant to a contract, sells a surveillance device to a local police department, the sale nevertheless may not be permitted by Section 2512. The suggestion is that under local law, the police department is not authorized to utilize the device in surreptitious electronic surveillance, the purchase by the police department is not "in the normal course of the activities" of the police department and so the sale is not sanctioned by Section 2512.

I do not believe the burden should be placed on the manufacturer in this way or that this is how Section 2512 should be read. I hope that this very serious question can be resolved, perhaps by a system that would involve the licensing of those permitted to possess and use surveillance devices.

In closing, on behalf of Bell & Howell, I want to express my pleasure at being invited to participate in these hearings and to pledge our continued full cooperation to your Commission.

MR. HERSHMAN: Thank you, Mr. Bower.

Mr. Holcomb, would you proceed with your statement, please.

TESTIMONY OF JACK N. HOLCOMB, PRESIDENT, AUDIO INTELLIGENCE DEVICES, INC.

MR. HOLCOMB: I would first like to express my appreciation for the opportunity to appear before this Commission and the forum it represents. The thoughts, ideas and recommendations which I would like to present will neither please my coun-

terparts in the manufacturing industry nor those concerned with abuse of existing law whose solution would be analogous to cutting off a man's head to cure his headache. However drastic they may seem to some or inadequate to others, these recommendations are not theoretical, visionary or hypothetical. They deal with the real world as it exists today.

In pursuit of solutions, we should recognize that the issues are often emotional and by human nature we tend to view one side of the coin without the other. The abuses have been well publicized. Watergate alone has received more lines in the news media and more actual television hours of coverage than all crimes, arrests and convictions that have occurred in the past twenty years. We cannot let this vast coverage of a single attempt at electronic intrusion give us permanent tunnel vision.

These are turbulent times, an area of extremes, both left and right; our position should be one based upon cold logic and reason and hard dispassionate consideration that is neither overly restrictive nor openly permissive. We must consider both individual rights and protection of the multitudes. I stress the majorities because the rights of the majority are entitled to consideration at least equal to the rights of the individual. Individual rights are important, but not so much so that a person or small group should be able to defeat, either openly or clandestinely, our entire system of government.

Unfortunately, our judicial system has evolved into a monster of technicalities in which guilt or innocence sometimes plays a secondary role. This inures to the benefit of the criminal because the courts, in their zeal to protect the rights of individuals, seem to lose sight of the rights of the majority of law abiding citizens. We must not let technicalities defeat the purpose of our laws.

The established policy of Audio Intelligence Devices, irrespective of legal restrictions, dictates that no equipment is sold to other than law enforcement agencies on the basis of regular purchase orders and paid for through the normal disbursement channels. We are not in the consumer marketing of products outside of law enforcement. Many of our devices could be lawfully sold to the general public; however, we have felt that to serve the needs of law enforcement as the major manufacturer in this field, we should restrict our efforts exclusively to this community.

Electronics and technical surveillance play an important role in the control of crime, yet it also must be held within the bounds of logic and reason. Our laws must be held within the bounds of logic and reason. Our laws must be sufficiently definitive to

make clear both what can and cannot be done. They should be neither vague nor ambiguous. The real practicalities have to be considered; and we must recognize that Utopia is not of this world.

Laws which will protect all individual rights as well as those of the vast majority are difficult to write. There will be some abuses as long as we deal with men. The more definitive we can make the gray areas, however, the less potential there is of honest error.

I would like to comment on the issue of honest error for this is a major problem in the law as it exists today. It is the gray area of no man's land. A law should never be passed which requires a Supreme Court ruling to clarify, in the minds of honest men, what was intended by the legislative body.

There have been some classic examples in Title III of this very issue. More than 400 convictions involving major narcotics sales were invalidated by the Supreme Court on the grounds that neither Attorney General John Mitchell nor his specially designated Assistant Attorney General signed the intercept authorization personally but, instead, he delegated this authority to a person not specifically designated in Title III.

This was not an intended abuse of the law; the Bureau of Narcotics and Dangerous Drugs, now DEA, believed their procedures to be correct. And who won and who lost when 400 narcotic dealers were turned loose to pursue their contemptible business? The winners don't sit here today; they aren't your friends and associates and those of you in Congress could not get an affirmative note from your constituency as approval for their release. Yet, in the name of error, some of the worst drug offenders were released. It was not a question of guilt or innocence, but purely a play upon a technicality in the name of individual rights.

For brevity, I am not going to read my entire statement.

CHAIRMAN ERICKSON: We certainly appreciate that, Mr. Holcomb. If you would endeavor to summarize it, I believe the Commission would benefit from it and it would facilitate our proceedings.

MR. HOLCOMB: I would like to recommend to the Commission that a new section be drawn to replace 2511 and 2512, and particularly 2510 and the definitions in it should be severely modified.

It should control manufacturer, sale, distribution, and it should specifically define the devices we are involved with.

There have been a lot of abuses in this field, abuses by manufacturers, by free-lance agents, importers, law enforcement, and uninformed citizens.

And the failure of the law to properly define prohibited devices and license and regulate manufacturers probably constitute two of the major deficiencies in the law as it exists today.

I have a number of recommendations for change.

CHAIRMAN ERICKSON: I think they are set forth in some detail in your opening statement, but if you could, just for the purpose of the record and for the purpose of cross examination, outline what those are, we would appreciate it.

MR. HOLCOMB: I would strongly recommend that statutes be drawn which would establish the Alcohol Tax, Tobacco, Firearms Division of the United States Department of the Treasury as the regulatory agency to license manufacturers, to establish serial numbers and record keeping; to license importers; investigate violations, and probably most important, promulgate administrative rulings for control and guidelines in furtherance of the statutes.

To add to what Mr. Bower had to say, this has been one of the gross problems we have faced. We have never been able to get anything in writing out of the Department of Justice as regarding administrative rulings, definitions, or how they would interpret any of the statutes. We are constantly told, upon query, that we must seek our own counsel. If we make a mistake and if we go wrong, they will indict us, and upon that indictment we will know we made a mistake.

I don't believe that this is the proper avenue to follow for any government regulatory agency. I think the Department of Justice was the wrong agency to have ever put this kind of a law under.

ATF is the logical agency to put it under. They deal with manufacturers in machineguns, and I specifically address my remarks to machineguns because the control of automatic weapons is very, very closely related in many aspects to the control of prohibited devices.

As far as control is concerned these laws must be rewritten. Manufacturers must be licensed. As Mr. Bower said, manufacturers must be able to manufacture efficiently and effectively without having to have an order first.

And I think more important, if you look at the administrative rulings of ATF as it regards automatic weapons, this is an agency that has had no hesitancy in the past to immediately say "Yes, you can do this," or "No, you can't do that," or "You can operate in this framework; that is as far as you can go. If you step over the line we will prosecute you. If you operate within the framework, you are within the law."

I think this is extremely important and this Commission could do one of the greatest services to the country by helping establish this.

I will present to the Commission within the next ten days to two weeks a proposed draft of the legislation and all the changes that would be required in Title III to implement a program that would change control and license manufacturers, importers, persons handling equipment, the sale of equipment, serial numbers on equipment, identification, and other means of implementing it through the Department of the Treasury and ATF.

I would hope the Commission would give substantial consideration to the recommendations that will be made in this law and the draft proposal that we will present to the Commission.

[The prepared statement of Jack N. Holcomb follows.]

STATEMENT OF JACK N. HOLCOMB,
PRESIDENT, AUDIO INTELLIGENCE DEVICES,
FORT LAUDERDALE, FLORIDA

I would first like to express my appreciation for the opportunity to appear before this Commission and the forum it represents. The thoughts, ideas and recommendations which I would like to present will neither please my counterparts in the manufacturing industry nor those concerned with abuses of existing law whose solution would be analogous to cutting off a man's head to cure his headache. However drastic they may seem to some or inadequate to others, these recommendations are not theoretical visionary or hypothetical they deal with the real world as it exists today.

In pursuit of solutions, we should recognize that the issues are often emotional and by human nature we tend to view one side of the coin without the other. The abuses have been well publicized. Watergate alone has received more lines in the news media and more actual television hours of coverage than all crimes, arrests and convictions that have occurred in the past twenty years. We cannot let this vast coverage of a single attempt at electronic intrusion give us permanent tunnel vision.

These are turbulent times—an era of extremes—both left and right; our position should be one based upon cold logic and reason and hard dispassionate consideration that is neither overly restrictive nor openly permissive. We must consider both individual rights and protection of the multitudes. I stress the majorities because the rights and protection of the multitudes. I stress the majorities because the rights of the majority are entitled to consideration at least equal to the rights of the individual. Individual rights are important, but not so much so that a person or small group should be able to defeat, either openly or clandestinely, our entire system of government. Unfortunately, our judicial system has evolved into a monster of technicalities in which guilt or innocence sometimes plays a secondary role. This inures to the benefit of the criminal because the courts, in their zeal to protect the rights of individuals seem to lose sight of the rights of the majority of law abiding citizens. We must not let technicalities defeat the purpose of our laws.

The established policy of Audio Intelligence Devices, irrespective of legal restrictions, dictates that no equipment is sold to other than law enforcement agencies on the basis of regular purchase orders and paid through the normal disbursement channels. We are not in the consumer marketing of products outside of law enforcement. Many of our devices could be lawfully sold to the general public; however, we have felt that to serve the needs of law enforcement as the major manufacturer in this field, we should restrict our efforts exclusively to this community.

Electronics and technical surveillance play an important role in the control of crime, yet it also must be held within the bounds of logic and reason. Our laws must be sufficiently definitive to make clear both what can and cannot be done. They should be neither vague nor ambiguous. The real practicalities have to be considered; and we must recognize that utopia is not of this world. Laws which will protect all individual rights as well as those of the vast majority are difficult to write. There will be some abuses as long as we deal with men. The more definitive we can make the gray areas, however, the less potential there is of honest error.

I would like to comment on the issue of honest error for this is a major problem in the law as it exists today. It is the gray area of no man's land. A law should never be passed which requires a Supreme Court ruling to clarify, in the minds of honest men, what was intended by the legislative body. There have been some classic examples in Title III of this very issue. More than 400 convictions involving major narcotics sales were invalidated by the Supreme Court on the grounds that neither Attorney General John Mitchell nor his specially designated Assistant Attorney General signed the intercept authorization personally, but instead he delegated this authority to a person not specifically designated in Title III. This was not an intended abuse of the law; the Bureau of Narcotics and Dangerous Drugs (now DEA) believed their procedures to be correct. Who won and who lost when 400 narcotic dealers were turned loose to pursue their contemptible business? The winners don't sit here today; they aren't your friends and associates and those of you in Congress could not get an affirmative note from your constituency as approval for this release. Yet, in the name of error some of the worst drug offenders were released. It was not a question of guilt or innocence, but purely a play upon a technicality in the name of individual rights.

What I am going to recommend to this Commission is a complete new section to replace Section 2511 and 2512 and additions to clarify other sections of Public Law 90-351. It will control manufacturers, sale and distribution, establish effective enforcement, specifically define prohibited devices, re-color the gray areas to black or white and bring the whole problem into realistic focus.

To address specifics, I will categorize my comments into three areas as follows:

(I) ABUSES OF THE LAW BY:

- (a) Manufacturers;
- (b) Freelance agents;
- (c) Importers;
- (d) Law enforcement;
- (e) The uninformed citizen.

(II) FAILURE OF THE PRESENT LAW:

- (a) To properly define prohibited devices;
- (b) To license and regulate manufacturers;
- (c) To incorporate categories of known abuse;
- (d) To establish standards for the industry;
- (e) To properly establish and fund regulatory enforcement.

(III) RECOMMENDATIONS FOR CHANGE:

- (a) Categorize devices as follows:
 - (1) intercept devices;
 - (2) officer protection equipment;
 - (3) entertainment items;
 - (4) alarm systems incorporating audio.
- (b) Establish Alcohol Tax, Tobacco, Firearms as a control agency:
 - (1) to license manufacturers;
 - (2) establish serial numbers and record keeping;
 - (3) license importation of prohibited devices;
 - (4) to investigate violations;
 - (5) to license industry and private individuals who possess controlled devices;

- (6) to maintain in central files exact specifications and identification of all prohibited devices;
- (7) to establish administrative rulings for control and guidelines in furtherance of the statutes.
- (c) Establish the National Bureau of Standards as agency for minimum standards;
 - (1) to establish minimum standards and certify equipment from manufacturers;
 - (2) to classify devices imported for private or industrial use;
 - (3) to furnish expert testimony when requested.

Let us stop pussyfooting around, hiding our heads in the sand, and recognize the industry as a legitimate tool of law enforcement, not the bastard child. Technology has come into its own and we can no longer ignore it as something that will quietly go away—it won't! There is a legitimate need that will genuinely serve the public interest but, like drugs, it can be for good or evil.

The Executive Director has been given copies of a proposed legislative draft which I believe would provide adequate safeguards and correct the problems that experience has defined. If the Chairman would incorporate these into my testimony by reference, it would better explain my own position in this matter.

Let's examine the abuses that have occurred under the present statutes. Who are the major offenders? Are they prosecuted and what are their penalties?

First, let's look at the manufacturers. Under the present law, manufacturers are totally uncontrolled. Not only does this lack of control inure to the inclination of abuse, but the law itself fails to set forth parameters which an honest manufacturer could follow. Manufacturers have sold equipment illegally or in a thinly veiled disguise of their own making. Since the manufacture and sale is related to devices "primarily useful for", any interpretation can be used as an excuse to move in almost any direction. As an example, infinity transmitters were sold as an intercept device and so advertised prior to the enactment of Title III. Now they are on the open market as an alarm system which permits the user, ostensibly, to telephone his office or home to determine if a burglary is taking place. This is pure farce. The infinity transmitter was designed as an intercept device and will always be used for that purpose notwithstanding any terminology as a burglar alarm.

It is axiomatic in this business that the smaller manufacturer, the greater the abuse. Why? Because in desperation, he is trying to make a living and the lack of volume alone defeats this purpose. He must resort to marginal interpretations for self-survival when the law fails in the form of hard definition.

The term "freelance agents" encompasses many categories of individuals. These include private detectives, security personnel, attorneys, unscrupulous politicians, telephone company employees, and numerous other persons. They are the major violators. Watergate is a perfect example. Although they were pursuing their targets with the knowledge of government, they themselves were employees of a private political campaign organization. They were not law enforcement, they held no official status and their acts were absolute violations of the law. There was no allusion as to the apprehension of criminals but purely and simply, an information gathering operation to be used for their own political gains.

Like manufacturers, importers are relatively unregulated and, because of the vagueness or total lack of present statutory definition, are free to ply their trade. They do this in the guise of wireless microphones for entertainment purposes, alarm systems, and other ostensible legitimate purposes. I am sure this Commission is more than adequately informed in this regard.

Abuses by authorized law enforcement agencies probably constitute the most minute group of offenses that have occurred since the passage of Title III. Honest mistakes have frequently been their most serious violation. Their purpose has been the

legitimate apprehension of the criminal element and in many cases the attack upon them has been based upon a court decision relating to the lack of probable cause which was all decided as a Monday-morning quarterback operation. It is always easy to determine that a mistake was made after all the facts are known. It is not as easy to gaze into that crystal ball with sketchy information and see a clear picture. It is interesting to note, however, that in the cases where the courts have held a lack of probable cause, the defendant was convicted of a criminal charge, and, the reversal related to the technicalities, not to the issue of guilt or innocence.

The uninformed citizen has been and always will be a common source of abuse as long as devices which can be used for illegal purposes are sold in the guise of legitimacy. This might be the individual who uses an automatic telephone recorder for the purpose of attempting to confirm his suspicion of misconduct of a business partner, associate, or wife. In the majority of these cases the citizen is not acting with willful criminal intent, but simply because he feels justified in his own mind that he has a right to know, particularly if he views himself as the victim, either real or imagined.

To discuss the subject of failure of the present law in its entirety would require a statement more lengthy than time in this instance would permit, and for this reason, I will touch only upon the highlights. The definition "primarily useful for surreptitious intercept" fails so completely that a manufacturer has difficulty operating legitimately within the law, even with a conscientious effort to comply. Anything is "primarily useful" for a purpose to which it can be adapted and so, we fall into a pit of semantics. This can be corrected in a manner which will permit a reasonably intelligent individual to comply with the intent of law without the merry-go-round of ambiguities that may only be resolved by Supreme Court decisions.

Title III does not license and regulate manufacturers. There is no coverage providing for research and development, inventory control, record keeping standards, possession by sales personnel, demonstrations to legitimate users, procedures of training law enforcement, or reasonable advertising to advise authorized users concerning available equipment. Title III as it regards manufacturers, is a classic of contradiction. It is both too restrictive and too permissive and serves neither master. Manufacturers must be licensed and controlled by established regulations. The law must be very definitive in this respect and should not indulge terms subject to a dozen different interpretations.

Categories of known abuse are not considered in Title III, such as wireless microphones. This is a typical example of an item that can be used by the movie or entertainment industry legitimately, but just as well by someone who wants to intercept the conversations by placing the device in adjoining rooms nearby. Some of these devices, when used with a good receiver and antenna system, can get a range of up to 1,000 feet or more. These areas must be properly defined in the law and provisions established for their control.

Standards for the industry should be established periodically by an agency of competent jurisdiction such as the National Bureau of Standards. A study should be properly made and minimum standards defined for all categories of devices to be regulated and controlled. It is ironic to note that there are more published standards on the common door bell than there are on the entire industry involving electronic intelligence equipment.

Title III names the Department of Justice for the purpose of regulatory enforcement. This is the wrong agency for the establishment of regulations in that they have neither the experience nor the machinery to indulge in such a pursuit. I will cover this in more detail in my recommendations for change.

My first recommendation is to establish, by category, electronic devices which would be used for the purposes of intercept by surreptitious means, officer protection equipment, entertainment items, and alarm systems which incorporate audio. These

four categories can encompass the classification of all equipment which has been involved in violations in the past.

I would strongly recommend statutes which would establish Alcohol Tax, Tobacco and Firearms as the regulatory agency to license manufacturers, establish serial numbers and record keeping, license importers of prohibited devices, investigate violations and promulgate administration rulings for control and guidelines in furtherance of the statute. If one makes a complete study of all U.S. government enforcement and regulatory agencies, the only conclusion that can be drawn is that the closest parallel to the devices in question and subject to these hearings, would be automatic weapons. Manufacturing problems are closely related. Serial numbering and record keeping are similar. Inventory control, possession for demonstration, and transportation are closely related. Transfer and sale are comparable. In no other government agency are these parallels present. ATF has the organizational machinery. They understand the problem of manufacturing, sale and distribution. They deal with serial numbers. They have competent personnel and they are widely respected by those whom they control as being legitimate enforcers of the law. They have a reputation of pursuing violations vigorously. They do not use their position as an ax and their integrity has been long established.

Controlled devices must require serial numbers that cannot be easily removed and records must be maintained that are traceable to permit identification of the purchaser. Possession licenses by manufacturing sales personnel should be established in the manner similar to the possession and handling of automatic weapons. Importation of devices relating to the four categories which I have previously mentioned must be licensed and regulated; they should require serial numbers and record keeping procedures similar to that of manufacturers.

Both intercept devices and officer protection equipment must be restricted to purchase by regular authorized governmental and law enforcement agencies only. Entertainment equipment and alarm systems incorporating audio must be industry controlled as well as licensed to the purchasers. Anything less will defeat the intent of the law.

Authority must be given to the control agency to establish administrative and procedural rulings in a similar manner to those issued by ATF in the control of automatic weapons. These administrative guidelines fill the void that is inadvertently omitted in the law or problems that were not contemplated at the time of legislation.

To effectively pursue control, ATF should be properly funded by Congress to employ experts in the specialized area involved and all necessary procedures promulgated by law to permit effective control and vigorous pursuit of violations. If they are to be given the responsibility then they must have the power to act. This should be clearly provided, not merely by assigning them the responsibility but to properly supplement them organizationally for adequate control of the problem.

An option that I would recommend would be the authorization and proper funding of the National Bureau of Standards for the establishment of minimum industry standards of technical definitions on an initial basis, and a review of those standards to occur at five year intervals. I would further recommend a procedure whereby ATF could call upon the National Bureau of Standards for expert testimony in prosecutions that would relate to statutory violations whenever ATF felt their experts were required.

I would like to pursue one final point because I feel it to be of the utmost importance in new legislation. That is the issue of single party consent. Legislation has been introduced eliminating recordings or interception by single party consent. Although I personally feel that if one is privy to or a party to any conversation, his constitutional rights would be violated by prohibiting him the opportunity to prove absolutely what he said or what anyone else said. In the area of law enforcement and successful

prosecution, this is absolutely a mandatory situation. It cannot be covered by court orders because the large majority of these situations occur on the spur of the moment. It is often the only means an officer has of protecting himself, without outside coverage, if he gets into trouble. It is often the only means he can employ to weigh the balance on the scales in his favor, in a criminal prosecution, when it becomes his word against the defendant's.

To eliminate single party consent is to prostitute truth. The police officer entitled to pursue the truth in the protection of the public interest by positively establishing the criminal's activities and intent. What better way exists to establish this than to allow the triers of fact to hear the evidence of criminal activity or intent in the voice of the offender? The constitutional question: whether a private citizen in the ordinary course of human events should have this right I would certainly not want to address. Laws which would permit the police officer this exclusive privilege, it seems to me, would pose no significant constitutional problem. It is absolutely mandatory that the law enforcement officer possess this option without restriction in the pursuit of his duties.

In conclusion, the final report of this Commission should serve both the public interest and law enforcement's effort to combat crime. Adequate laws can be written which will serve these needs. Your recommendations will weigh heavily toward this end. If the pursuit is one that recognizes the problems, as a practical matter, correcting the ills without losing the patient, you will have accomplished your goal.

CHAIRMAN ERICKSON: Mr. Holcomb, we appreciate that very much.

I might suggest when you indicated that Title III was not perhaps the greatest picture of clarity, that Professor Blakey on this Commission was the primary draftsman, so I am sure he will have a few questions on that issue.

Mr. Morrissey, do you have an opening statement?

TESTIMONY OF MICHAEL J. MORRISSEY, FORMERLY OF B.R. FOX COMPANY, INC.

MR. MORRISSEY: Thank you, Mr. Chairman. I will keep my opening remarks brief.

Mr. Chairman and members of this Commission, these hearings commencing today and continuing for the next two days are of extreme importance and significance. I want to express my appreciation to the Commission for allowing me the opportunity to appear here and contribute in this effort.

The first Congressional review of a new federal law is significant in itself, but this takes on added importance for it was under extreme circumstances that gave birth in 1968 to Title III of Public Law 90-351.

The importance of these days are accentuated in a legal sense in that this only concerns a federal law but it touches upon a constitutional right of the Fourth Amendment, and as such lies within the zone of close scrutiny.

But the importance of these hearings is paralleled by the uniqueness of the subject matter, for it is a by-product of an electronics industry so diverse and active that the state of the art is routinely giving way to newer developments.

It is unique in a social sense because this subject does not direct itself to any minority group, any particular segment of America, or to a vested interest group, but rather it has the potential to touch and concern every American.

The technology advanced rapidly during the past 20 years from vacuum tubes in the Forties to transmitters in the Fifties, to integrated circuits and micro-miniaturization in the Sixties, and it was in this atmosphere that the two landmark decisions of the Supreme Court of the *United States v. Katz* and *Berger v. The State of New York* served as a foundation for the enactment of the present legislation. But the industry has continued to spiral and it is demanding of the law, if not outright control, at least clear definitive guidelines. Even basic definitions are now outdated or at least need clarification.

Examples include the term "electronic surveillance" which at one point in time implied audio intercepts. Today we have data banks, digital transmission and a host of other loopholes around electronic surveillance or another definition, "electronic audio surveillance."

Another term running through the present law is "wire and oral communications."

This is a mixture of a mode of carrier with a mode of communications.

Hence, the radio frequency transmission of digital data might not necessarily fit under the heading "wire" or "oral" communication.

But the primary phrase that affords, at least in my mind, the greatest amount of confusion is the definition of the equipment and devices that are sought to be controlled by the law:

"The design of such device which renders it primarily useful for the primary purpose of surreptitious interception of wire or oral communications." I believe this is the phrase that needs the greatest amount of clarification.

The present law provides for the use of this equipment in two circumstances: One controlled by law enforcement; another uncontrolled by non-law enforcement under certain circumstances, namely when you are a party to the conversation. But the possession of the equipment is closely restricted in stating that you first must be under contract.

An analogy exists in this sense to the plight of the prostitute in France where prostitution is allowed but soliciting is illegal. So, too, use of the equipment is permitted. Its possession, however, is against the law.

I cannot share the enthusiasm of my colleagues at this time with the idea of licensing as a solution. We must first direct ourselves to defining clearly and unambiguously that which we seek to control, namely a device primarily designed for surreptitious listening. This raises serious problems in view of the commercial products now available.

Unlike in other fields, such as alcohol where a quantitative definition is possible, or in firearms where a gun is a gun and nothing else, electronic surveillance equipment covers a broad spectrum of the electronics field.

We are talking of a situation where a screwdriver can do much more harm than a sledge hammer. And how do you control implements of this activity?

The closeness of commercial products to the devices we seek to control is exemplified by the fact that only \$10 worth of parts can convert almost any radio or T.V. speaker into a surreptitious listening device.

To characterize a single item standing alone is over-restrictive in the eyes of free trade, over-burdensome in the eyes of the manufacturer, and I feel over-broad in the eyes of the law.

There is also confusion in the term of advertising. The current law states that this equipment cannot be openly advertised. At the last convention of the largest national police organization, this equipment was not allowed to be shown not only on the manufacturers' convention floor, but neither in a room where only law enforcement personnel were allowed.

The confusion is exemplified by the fact that the telephone yellow pages will not accept an ad for counter-measure services for wiretapping detection. Yet a store in Washington openly advertises across its windows "electronic surveillance equipment", and on 42nd Street in New York a store displays devices that draw the curious and the serious.

There is one more concern, one that can never be resolved by modifying the law or writing a new law. Yet it over-shadows all the rest. This is the present concern about the present attitude and confusion of not so much those within the field but of the American public toward an activity suspiciously known as electronic surveillance. It is my hope that the information exchanged here will be transmitted into a more informed public, a more effective police force and a more workable law in a recognized and accepted field.

CHAIRMAN ERICKSON: Thank you, Mr. Morrissey.

Before having the staff commence the interrogation, I would judge from the remarks that you have made that you think there could be some clarifying legislation.

MR. MORRISSEY: Yes, Mr. Chairman, I feel so.

CHAIRMAN ERICKSON: Mr. Hershman.

MR. HERSHMAN: Mr. Bower, I wonder if you could tell the Commission what procedures you use to ensure prospective purchasers and customers are authorized to purchase your equipment?

MR. BOWER: Yes, sir, Mr. Hershman. Perhaps the best way to do that would be to pursue a typical sale from its inception and how it comes about and the controls that we institute in that area.

First of all, a law enforcement agency, in order to obtain one of our catalogs, is required to write his request on a Department letterhead. This request must be signed by the senior officer of the group. And this request must come to my desk personally. And I personally authorize the release of our Special Operations catalog to that agency.

This particular catalog is, of course, controlled. It is serially numbered. We maintain a log of the distribution of these documents, and this log also is maintained under my personal supervision.

At that point, upon perusal of the document, if the agency wishing to purchase the equipment makes a decision of interest then typically, for example, in Massachusetts he would communicate with me or with my Massachusetts salesperson and indicate a desire to discuss prospective purchase of the equipment. At that point a personal call would be made on the agency or on the officer involved by my salesman and in the official's office the equipment would be presented and discussed, and the needs of the agency or department discussed and the equipment best applied to those needs would be recommended by my salesperson.

Again, if the official's decision was in the affirmative to pursue the purchase of such equipment, this purchase would take the form of a formal purchase order, again on the stationery of the department or the agency, that is to say, a bona fide purchase order, and that presumably would be transmitted again and must receive my personal approval before release to manufacturing.

So we feel, as a result of all these internal controls, that we are confident that, number one, we know where every single document describing our equipment physically rests, or at least where it rested when it left our premises; and we also know where every piece of equipment has gone that we have sold.

MR. HERSHMAN: So then, Mr. Bower, if a police officer walked into your office and showed you a shield or a badge, he could not purchase equipment on the authority of that badge or shield?

MR. BOWER: That is correct. No, we would need absolutely a formal purchase order from the officer's department. We accept no verbal orders, Mr. Hershman.

MR. HERSHMAN: And do you require that a senior official in the department sign the purchase order?

MR. BOWER: Not necessarily in the department but a senior official in the agency. That is to say, police departments have various units, and I would accept an order or a request for a catalog from a senior officer of the unit.

Purchase orders ordinarily, especially in larger groups, are signed by the city comptroller or other financial officer of the city.

MR. HERSHMAN: Mr. Holcomb, could you tell us how often you are approached by unauthorized people to purchase equipment that is designed for the surreptitious overhearing of communications?

MR. HOLCOMB: We receive requests on the average of three or four a week from those not connected with law enforcement agencies. In some cases we don't know whether they are connected or not with an authorized law enforcement agency. We answer that with a stock, standard form letter that says in effect, "We do not sell to anyone other than authorized law enforcement agencies," and, "We are terribly sorry," and that, "You should pursue your endeavors elsewhere."

We don't have many phone calls—occasionally, but not that many. Mostly these are requests in writing.

Some of them are from high school students who want catalogs because they are doing a research paper for a school project. Some of them are college people for the same reasons. Rarely do we get anything from a private detective. It is mostly all individuals. It is individuals; it is attorneys; it is school children—people that fall in this category.

MR. HERSHMAN: You say you get letters from attorneys requesting to purchase electronic surveillance devices?

MR. HOLCOMB: For catalogs. We send them the same form letter we send a school kid.

MR. HERSHMAN: In these letters do they indicate what their intention is as to the use of the equipment?

MR. HOLCOMB: No.

MR. HERSHMAN: The phone calls that you receive—are the people persistent? If you won't sell them the equipment or give them the catalog, do they ask you to recommend someone who will?

MR. HOLCOMB: Yes, quite often they will do this. Our answer is that we do not recommend anyone; that they would have to pursue through their own endeavors and their own efforts a source. Quite often they get bent out of shape with us because they are requesting something which is not in any way a prohibited device.

For instance, we use an enormous number of Uher recorders. We stock all parts and all repair parts and components for Uher recorders. We get calls sometimes from the news media who say "We want to buy a new motor for our Uher recorder."

Our policy is we don't sell anything except to law enforcement agencies, and we turn them down so we get some flak that others might not.

MR. HERSHMAN: In your opening statement you indicate you have knowledge of manufacturers who have sold equipment illegally. I wonder if you could tell us the circumstances surrounding those illegal sales.

MR. HOLCOMB: Well, I know equipment of different types shows up in different places. What the circumstances surrounding the sale amounted to, I couldn't say, because I wasn't there when the sale took place.

But I know there is equipment that shows up in places that it shouldn't show up.

MR. HERSHMAN: For example, sir?

MR. HOLCOMB: Are you speaking about the design of equipment or specific equipment?

MR. HERSHMAN: I am speaking about the equipment you referred to in your opening statement as being sold illegally in the United States.

MR. HOLCOMB: Well, first we go back to Section 2510, No. 5, which, by definition, states that electronic, mechanical or other device means any device or apparatus which can be used to intercept a wire or oral communication.

This can be used as an all-encompassing term to include every tape recorder ever made, including the Nagra I think he has sitting over here on the table.

This is a type of situation that puts us into such an encompassing statement, and devices are by the manufacturers, themselves, determined as to whether they are illegal or not. There is an ad openly for body transmitters in magazines, for example. These are sold on the open market. And the infinity transmitter.

If any device can be used for surreptitious intercept, it certainly has to be these.

MR. HERSHMAN: And are you aware of any prosecutions for the sale of these illegal devices?

MR. HOLCOMB: No. In several devices where an illegal sale was to take place, we did notify the Department of Justice because an approach in one instance was made to one of our people to handle such equipment and buy it on a speculative basis. We knew this to be a specific violation. We did report it to the Department of Justice and to the FBI, both. As a matter of fact, there was a meeting set up with the man in which we told the FBI, "If you want to come and record the meeting, we will give

you the consent. You come and listen to the pitch and look at the literature and you tell us what it is."

Nobody ever showed up. It just gets dropped right there.

I bitterly complained about some of the things that manufacturers do, for instance putting equipment in the frequency range of 113, 115, 118 megaHertz. This is an aircraft guidance band. This should be an offense the likes of which prosecution should be pursued instantly.

MR. HERSHMAN: What you are suggesting, then, is that this equipment might broadcast in a range which might interfere with ground-to-air communications?

MR. HOLCOMB: For instance, when you take equipment in this area in your guidance bands, if an airplane is approaching an airport—such as the crash that occurred on the Eastern plane—and somebody has a device putting out a half watt near the airport, it could bring it in substantially short of the runway, particularly in bad weather and on instrument approaches. So equipment should never be put in the aircraft guidance band. It is a hazard to the public that far exceeds anything that we have ever seen in this field.

Yet it is openly advertised, and the literature even states "a half watt above 112 megaHertz, in the aircraft guidance range."

I have complained to FCC about it; I have complained to Justice about it; I have complained to Mike Hershman about it. But it doesn't seem that anybody is willing to do anything about this problem. And it is a severe problem. If people knew that equipment not crystal controlled was put in an aircraft guidance band they would be afraid to get on an airplane.

MR. HERSHMAN: Thank you, Mr. Holcomb.

Mr. Morrissey, there seems to be a problem interpreting a phrase "a device which is used for surreptitious interception of wire and oral communications."

I wonder if you could describe to us, including some of the devices you have sold in the past, which devices may fall into the unclear region.

MR. MORRISSEY: Mr. Hershman, I think this is the major point in the law that needs clarification. I appreciate it being brought up at the outset.

Devices that would fall into the unclear area would be, for one, a basic body transmitter; and, number two, a telephone recording device, both of which are commercially available, sold in radio stores at far less price than police departments are paying.

The law provides for the use of this equipment by a person who is a party to the conversation. The major networks use pocket transmitters frequently for on-the-street interviews.

The TV and stage industries use pocket transmitters for remote stage transmission .

Telephone answering equipment, available in department stores, frequently has an adaption for recording telephone conversation to refresh one's recollection, let's say, if they are in a stock brokerage business, or else at times as a defense to the person being called, which is also supportive of the court's best evidence rule.

So I find it difficult at the outset to see exactly what it is that we are trying to control.

Now, let me give an example of the other extreme, a device that I would characterize as primarily designed for surreptitious listening. That would be something like a harmonica bug, designed to be planted in the phone, designed to be remotely activated secretly, or a transmitter built into an AC wall socket, where you have to do a more or less permanent installation.

Even letting your imagination run, it is hard to find a legitimate use for these types of devices.

But in my experience, the greatest demand from law enforcement is for the basic transmitter unit and a basic telephone recording device. And both of these, I feel, fall into the category of ambiguous when related to the definition in the law.

MR. HERSHMAN: Mr. Morrissey, would you say with the advent of integrated circuits and miniaturized components it makes it all the more difficult to interpret what is primarily designed and what isn't?

MR. MORRISSEY: Most definitely. As an example of this, the law enforcement departments have sought for a number of years now a good, very miniature body tape recorder, something that can be worn secretly on the person. Yet it hasn't been available—a real dependable unit in terms of law enforcement. But the commercial market has produced this and produced it much better and much smaller than we have done.

And, in fact, there is a cassette tape that has been developed and I understand will be released within the next six months which is one-third the size of the standard cassette today. And it will give one hour of recording on one side.

Now, this is going to be a product that is in demand by law enforcement groups for surreptitiously recording another conversation. Or it may be used by a person when they are a party to the conversation, but it will most definitely be used by the business community as a standard piece of office equipment.

Now, how do we categorize that device?

MR. HERSHMAN: Thank you, Mr. Morrissey.

Mr. Bower, in your opening statement you seemed to indicate that Bell & Howell considers

wiretapping a far greater possible area of abuse than bugging. I wonder if you would explain that for us, please.

MR. BOWER: Yes, I'd be pleased to, Mr. Hershman.

Sometime ago a corporation decision was made not to manufacture equipment useful for wiretapping. The feeling was, as I understand it, at the time that wiretap equipment lent itself to non-consensual intercept in a much broader sense than oral intercept equipment did.

So, as I indicated earlier, in my opening statement, there was a corporate decision made not to manufacture wiretap equipment, largely for that reason.

MR. HERSHMAN: Thank you.

Mr. Holcomb, we discussed a short while ago the approaches of unauthorized individuals in order to purchase equipment or gain one of your catalogs. I would like to know if you know of any instances where a law enforcement or official letterhead was doctored in order to purchase or receive electronic surveillance equipment.

MR. HOLCOMB: Yes, there was a recent situation that occurred in San Francisco. This did not occur with us. I understand it occurred with two or three of the other manufacturers.

MR. HERSHMAN: And what happened there, Mr. Holcomb; do you know?

MR. HOLCOMB: As I recall, we were warned well in advance of this situation, so we did not fall into it and no approach was made to us. But basically it was a situation where a letterhead was designed to read something like "The San Francisco Bay Area Narcotics Strike Force"—something to this effect. And I understand that this particular situation did exist with a couple of manufacturers. They did ship equipment and then found out it was a phony address, post office box, and it is under investigation at this time.

MR. HERSHMAN: So that there are manufacturers who will ship equipment on the basis of a simple letterhead, never having contact with the individuals signing the letter or purporting to be with that agency; is that correct?

MR. HOLCOMB: There is no question about it. The smaller manufacturers, particularly the one- and the two-man operators, quite often fill orders based on letters—law enforcement or otherwise. And they don't have the procedures nor the facilities to check these things out.

We will not accept a letter as an order from anybody.

MR. HERSHMAN: Mr. Bower, according to your interpretation of Section 2512, you cannot maintain an inventory or conduct research and

development on electronic surveillance equipment because you feel you cannot build it without a contract with a law enforcement agency?

MR. BOWER: Yes, that is correct. We have not had any new products for a number of years for this reason. And we consider this rather a disservice to the law enforcement community. And, as you mentioned in your first sentence, we do not manufacture for inventory and we feel this is a very serious detriment to the law enforcement community's efforts to do their job, in view of the fact that if they have a serious need in a certain area and a need for equipment and place an order on us, we have to start virtually from zero to manufacture that equipment for them.

MR. HERSHMAN: Can you tell us how this affects the price of the equipment to law enforcement and the time of delivery?

MR. BOWER: Yes, sir, it affects it very adversely.

In the first place, our costs are obviously inflated because our suppliers can only furnish the components in the quantities we order, and since we order for a controlled inventory it is necessary to order from our suppliers of components only enough pieces to fill current orders. We are not able to order parts, obviously, for a year's projection of material.

Naturally, when you order in small quantities you sort of get behind all the larger orders with your supplier. He is anxious to fill his large orders first and the small order comes second, and the cost is accordingly higher.

MR. HERSHMAN: Mr. Bower, would it not be feasible or possible to build the equipment leaving out an integral component, thereby rendering it ineffective and add that component when the equipment is sought for purchase?

MR. BOWER: Yes, that is certainly possible. Whether that is a wise decision or not, I am not sure—depending on which component was left out. You could go pretty far in a piece of equipment and then make it operational by the purchase of an uncontrolled device, such as Mr. Holcomb has suggested, such that if the device was complete except for its microphone, for example, you could buy the microphone in any radio store and that would not allow us the kind of control we feel is necessary in compliance with 2512.

MR. HERSHMAN: Mr. Morrissey, Mr. Holcomb feels that foreign sales of authorized equipment should be authorized. Do you agree with Mr. Holcomb?

MR. MORRISSEY: Would this include transmitters?

MR. HERSHMAN: I am primarily talking of devices which would be prohibited under 2512.

MR. MORRISSEY: I feel that foreign sales could best be handled by going through a controller office such as ATF.

MR. HERSHMAN: Do you feel these sales should be limited to certain countries?

MR. MORRISSEY: Well, this would be up to the controlling office that is handling the exportation of the equipment. And no doubt this would come into play in getting the proper authorization to make the sale to a foreign request.

I could differentiate this, however, from domestic sales in seeing that the intent in keeping these devices out of certain foreign hands is more obvious and apparent, and hence the need for some export control.

Internally, by using the present set-up we have, operating with a proper law enforcement agency takes care of this central control.

MR. HERSHMAN: Mr. Morrissey, we have examined the records of the firm that you were formerly associated with, as well as the records of Bell & Howell and Audio Intelligence Devices and those of six other manufacturers' firms in the country.

We have noticed that your records, as well as all the others, reflect sales of equipment which is primarily useful for the surreptitious interception of wire and oral communications to police departments in states without authorization statutes.

Do you try to make any determination as to whether a police department can legitimately use this equipment or not?

MR. MORRISSEY: No, Mr. Hershman.

I think to require that of the manufacturer would be overly burdensome. It would necessitate him to be familiar with not only the letter of the law in each state, but also the court's attitude towards the field and the recent decisions in this area.

I believe there should be control in this area, but I don't think it should rest with the manufacturer.

MR. HERSHMAN: Do you believe that the responsibility for obtaining and purchasing the equipment and the use of it should lie, then, in the hands of the police departments who sought to gain the equipment?

MR. MORRISSEY: In terms of whether or not their state allows them to use that equipment?

MR. HERSHMAN: Yes.

MR. MORRISSEY: Yes, I do.

MR. HERSHMAN: Mr. Bower, I would like to address the same question to you. Do you try to make any determinations as to whether a police department is authorized to have the equipment or not?

MR. BOWER: No, Mr. Hershman, we do not. It is regrettable that the media has made a sort of blanket indictment against a number of states which apparently do not have enabling legislation.

The documentation of this legislation is a massive volume, and as Mr. Morrissey indicated, for a manufacturer to be current on the spirit and letter of statutes in all the jurisdictions with whom we deal is pretty much of an impossibility.

Therefore, we concur with Mr. Morrissey's statement that the responsibility for lawful use does rest with the end user, especially in view of the fact that the equipment that at least we manufacture has other uses, outside of 2512, which are very beneficial to the law enforcement community, particularly in the areas of protection of officers and in training.

MR. HERSHMAN: Now Mr. Bower, you bring up the matter of training. I understand that Bell & Howell conducts training courses for police officers in the use of electronic surveillance equipment; is that correct?

MR. BOWER: Yes, that is correct.

MR. HERSHMAN: Do you make any distinction between the police officers who come from states without authorization statutes and those who come from states with authorization statutes?

MR. BOWER: Yes, we do. We draw to the attention of the students in our training seminars that their state does or does not have enabling legislation. We provide them an opportunity to peruse this legislation as part of the training and we encourage them to make certain that the equipment that they use in their home department be used lawfully at all times. And our thrust in that area is to encourage and promulgate lawful use, and we do bring to the attention of officers from each state, as I mentioned, the legislation in that state.

We do not attempt to interpret it.

MR. HERSHMAN: Mr. Holcomb, Audio Intelligence Devices is co-located with the National Intelligence Academy which is set up as I understand it to instruct police officers across the country in the use of electronic surveillance devices. I understand you are a consultant to the National Intelligence Academy; is that correct, sir?

MR. HOLCOMB: That is correct.

MR. HERSHMAN: Could you tell us what type of training is offered to these police officers across the country?

MR. HOLCOMB: A basic course in electronics and the application of it; quite an extensive course in the legality section.

The basic course is not designed so much based on equipment but as to the principles of how equipment operates. So the Officer that spends two weeks in training on such a course would at least know what such a piece of equipment might or might not do under field conditions and the reasons for failures.

Basically it was set up for the purpose of trying to cut those failures down.

MR. HERSHMAN: I understand the Academy does give instructions on wiretapping and bugging. I understand there is a room set up to instruct the attending students on where to place a bug and how to install it.

Is that correct, sir?

MR. HOLCOMB: Yes, sir.

MR. HERSHMAN: Do you distinguish between officers coming from authorization states and those coming from non-authorization states?

MR. HOLCOMB: No, the school does not, and neither does AID.

As far as Audio Intelligence Devices is concerned, and our position regarding the headlines of police purchasing bugs in states that forbid use, such as appeared yesterday, I think this is a gross disservice to the American public. I think it misleads people grossly in the idea that there is some nefarious scheme in these departments buying devices.

Now, unlike Bell & Howell, we do sell and manufacture equipment that falls in this category. We do sell it in states that do not have an enabling statute. But also, these states do have consensual conditions, and the percentage of hard intercept devices as opposed, for instance, to officer protection equipment, is very, very small. And the departments who buy items generally buy one or two at the most. And they are buying it for the consensual situations in terms of the kidnap cases, the extortion cases, the narcotics cases, where they have a consensual situation to use that equipment and they do have a legitimate use for it, notwithstanding the fact that there is no enabling statute in their states.

MR. HERSHMAN: I believe, Mr. Holcomb, quite a number of wiretap and bugging devices are being purchased, by agents and departments in non-authorization states, more than ever could be used for kidnaping or murder or extortion in any of these states.

MR. HOLCOMB: I don't agree with that, Mr. Hershman, at all.

MR. HERSHMAN: I would like to say the National Wiretap Commission requested through you at one time the records of those students attending the National Intelligence Academy. Those records were not forthcoming. Nevertheless, we managed to obtain them.

And our records show that attending your school, 70 out of 224 students, making it 31.2 per cent, are from non-authorization states and they are there to learn wiretapping and bugging and not only consensual monitoring, and I just don't see the reason for this. Perhaps you can explain.

MR. HOLCOMB: I think to begin with you place the emphasis on wiretapping and bugging. The emphasis in the school is not placed on wiretapping and bugging because the main use of equipment in this field today—and make no mistake about it—is in consensual situations, and principally under officer-protection conditions.

Now, in some cases equipment is used in narcotics situations, particularly as it involves informants; undercover people in which, for instance, wall transmitters or telephone drop-in transmitters are used. But if you look at the percentage of equipment purchased by any law enforcement agency where there is no enabling statute, you will find the devices purchased for officer protection and consensual situations far, far exceed in percentage the devices that are purchased that would be hard intercept devices.

MR. HERSHMAN: I think that is absolutely correct. I worry about the minority of the devices purchased by the police departments.

You expressed particular concern about foreign export of these devices.

I would like to know, Mr. Holcomb, if your products are sold exclusively under the name of Audio Intelligence Devices.

MR. HOLCOMB: They have been in the past. We have established another name which will be used in the foreign market and that name is Technos International.

MR. HERSHMAN: Technos International?

MR. HOLCOMB: Yes.

MR. HERSHMAN: Have there been any sales of equipment through Technos International to date?

MR. HOLCOMB: That is just being set up now. I think there have been a couple of shipments of equipment but none that fall in the category of surreptitious intercept as would be prohibited in foreign commerce.

MR. HERSHMAN: Who has determined what the category is? Is that your determination?

MR. HOLCOMB: I think we probably are in a better position to make determinations than anybody else.

For instance, if we ship receiving equipment, I don't think there can be any question in anybody's mind as to whether receivers constitute an intercept device. Because if that is the case and if receivers do in fact, then I am sure everybody in this room is guilty of violation of the law.

MR. HERSHMAN: So Technos International has been involved in sales only of devices which are not primarily useful but rather devices which would fall outside of the prohibition in 2512; is that correct?

MR. HOLCOMB: That is correct.

MR. HERSHMAN: Thank you.

Mr. Holcomb, getting back to the question of licensing, do you really believe that licensing manufacturers would tend to drive out your basement operators, as they are called, your illegal operators?

MR. HOLCOMB: Mr. Hershman, I don't think you can control any industry if you don't control the manufacturers. And I think manufacturers should be required absolutely to put serial numbers on the equipment that cannot be removed so that violations—when a piece of equipment is found, at least it can be identified and traced back to the original purchaser.

This is one of the major problems that occurs today.

Now, you are not going to be able to affect this kind of situation unless you have hard penalties, and they are probably going to have to be mandatory penalties where you have a minimum sentence of a year or of two years for anyone convicted of a violation. I think your minimum sentence is going to have to be absolutely essential to control this situation in the long haul.

MR. HERSHMAN: Mr. Morrissey, can you perhaps tell us the approximate percentage of your equipment purchased by police departments through the use of LEAA funding?

MR. MORRISSEY: I would have to estimate this. It is certainly a majority. Since 1972 I would estimate 75 percent.

MR. HERSHMAN: So then can we assume, Mr. Morrissey, that some of the equipment purchased by police departments in states without authorization statutes were purchased through the use of LEAA funds?

MR. MORRISSEY: You might assume that. I don't think that as a manufacturer I am in a position to state one way or another on that.

MR. HERSHMAN: But that possibility does exist, does it not?

MR. MORRISSEY: The fact that LEAA funds local police departments to purchase equipment, and the fact that police departments can purchase equipment using either in part or in total LEAA funds raises the possibility that that could be a true statement, yes.

MR. HERSHMAN: Mr. Morrissey, do you know of any policy on the part of LEAA to restrict purchasers of this equipment to police departments in states with authorization statutes?

MR. MORRISSEY: No, I don't.

MR. HERSHMAN: Thank you.

Mr. Bower, again getting back to your interpretation of 2512, according to that interpretation it seems that you believe the display and demonstration of your equipment would be forbidden. Is that correct?

MR. BOWER: Yes, sir, that is accurate.

MR. HERSHMAN: How do you get a police department to purchase your equipment if they have never seen it work?

MR. BOWER: As I mentioned earlier in my discussion of how a sale was conducted from its inception to its conclusion, I think I indicated one of the first steps would be a police department or law enforcement agency requesting one of our catalogs and then specifically requesting a demonstration at that point.

I think I covered that fairly extensively when I discussed the sale.

MR. HERSHMAN: And you believe you should be able to display and demonstrate your equipment without a contract between yourself and law enforcement; is that correct?

MR. BOWER: Yes, that is correct, Mr. Hershman; yes.

MR. HERSHMAN: Mr. Holcomb, I would like to ask this. The Commission is currently studying the state of the art of electronic surveillance technology. And we have seen many advances since 1968 in the design and implementation of devices. Can you tell us a little of the future, of what we can expect in technological advancement?

MR. HOLCOMB: I think you are going to see an enormous advancement come out of technology in this field. I suspect it is going to be principally by the few who do commit substantial R&D into it.

We, unlike Bell & Howell, do have a very, very substantial research and development commitment. And we are pressing it hard. We do not feel that we are committing any violation.

And I think in the coming years some of these advancements in this area are going to be considerable. There are some areas of devices which haven't changed basically in the last ten or 15 years, the reason being that you are faced with a battery situation. The technology of batteries has not advanced that much. And in most instances, particularly in body-worn equipment, your batteries are from three to five times the size of the device they are used with.

So, as long as you are faced with a situation where you can't reduce the size of the batteries, then what good does it do you to get the equipment down to an ultra-ultra-miniaturization?

MR. HERSHMAN: Mr. Holcomb, if I understand you correctly, you do not believe your research and development is illegal under the statute?

MR. HOLCOMB: No.

MR. HERSHMAN: What about display and demonstration?

MR. HOLCOMB: We display and demonstrate to law enforcement agencies upon their request—only to them. We produce equipment. We inventory equipment.

MR. HERSHMAN: You inventory equipment?

MR. HOLCOMB: We inventory equipment that is probably up to 90 per cent completion. Maybe we don't have the crystals in it; maybe we don't have some other things in it. We have crystals burned in separately because crystals require days to burn in.

I think I would be remiss in my duty to law enforcement if I was not in a position to supply equipment immediately for major operations—when I say "immediate," possibly the same day or next day. I think this is mandatory.

MR. HERSHMAN: How many sales personnel do you employ in the United States?

MR. HOLCOMB: Approximately 12.

MR. HERSHMAN: And are they in possession of equipment which is used for demonstration and display?

MR. HOLCOMB: Yes, they are.

MR. HERSHMAN: You do not consider that contrary to the current law?

MR. HOLCOMB: No, I do not.

Now, I will say this. At all times we have a sufficient number of orders pending in house to cover every piece of equipment we've got.

MR. HERSHMAN: I don't believe that was the intent of the law.

MR. HOLCOMB: I don't believe the intent of the law was to stop a manufacturer from doing something in an efficient, honest and legitimate manner.

MR. HERSHMAN: Mr. Morrissey, what can you tell us about the importation of electronic surveillance devices into this country and the components which are main ingredients of these electronic surveillance devices?

MR. MORRISSEY: As far as the importation of this equipment, I have discovered that there is equipment that is being sold through wholesale outlets in this country, and there is definitely literature that will come into this country from outside sources.

This even goes down to the level of the local radio store where some of such devices have been brought to my attention from an outside source and of course this is beyond our jurisdiction except for the person within the United States, should they decide to go ahead and purchase this.

But the fact that foreign manufacturers may solicit business within the United States—this has been brought to my attention more on the commercial market actually than in the law enforcement area.

Now, as regards components, this is a difficult area because thousands and thousands of components are imported into the United States for use in a variety of electronic devices and electronic

equipment. And so at the same time they are imported, it is impossible to determine their end product in which they would be used.

MR. HERSHMAN: Thank you, Mr. Morrissey. Thank you, gentlemen.

CHAIRMAN ERICKSON: Mr. Bower, you have suggested that the records of your company are such that you can tell where every piece of equipment that would fall within the Act has been sent; is that correct?

MR. BOWER: That is correct, sir.

CHAIRMAN ERICKSON: Are those pieces of equipment identified by serial number?

MR. BOWER: Indeed they are, Mr. Chairman.

CHAIRMAN ERICKSON: So if at any later time a device was found, you could trace that device?

MR. BOWER: We feel confident we could locate the original purchaser.

CHAIRMAN ERICKSON: Mr. Holcomb, is that true regarding the devices you manufacture?

MR. HOLCOMB: Yes, sir. We serial number it and play games with other types of identification so if the label or serial number is ripped off we can still identify it.

CHAIRMAN ERICKSON: When you say "play games," you mean you utilize other means such as automobile manufacturers do, to maintain the identity of their automobiles?

MR. HOLCOMB: That is correct.

CHAIRMAN ERICKSON: Mr. Morrissey, what was your experience in this area?

MR. MORRISSEY: Mr. Erickson, I don't serialize devices. Unlike Mr. Bower and Mr. Holcomb, my operation is somewhat different and I think it is representative of a large number of suppliers in this country.

I deal on a very personal level and close level with the law enforcement groups that I either train or supply equipment to, and my equipment would be identifiable to me only in terms of its external appearance.

CHAIRMAN ERICKSON: Thank you.

Mr. Holcomb, in your opinion would elimination of consensual electronic surveillance within the law—except for law enforcement purposes—help solve the problem of what is a prohibited device?

MR. HOLCOMB: Mr. Chairman, would you repeat that question again, please?

CHAIRMAN ERICKSON: Would elimination of the consensual electronic surveillance provision in the Act, except for law enforcement, help solve the problem of what is a prohibited device?

MR. HOLCOMB: Yes, I think you could solve a lot of problems by that. Whether you would create some others of a constitutional nature or not, I don't know. But that would be for the courts to pass on.

I do believe that the consensual situation that is employed by law enforcement is as mandatory as the policeman, himself. And I think that if any law were passed which eliminated single-party consent in the United States, you would literally put law enforcement out of business.

CHAIRMAN ERICKSON: I am not condemning the use of consensual eavesdropping equipment by law enforcement but I am questioning whether or not it should be available to every member of the public.

MR. HOLCOMB: I don't believe, Mr. Chairman, that the equipment, other than possibly a standard tape recorder, or the ordinary things along this line, should be available to the public. I don't think, for instance, that wireless microphones should be available on the market to the public uncontrolled. I think they should be controlled. And I think some agency of government should know where they go and who buys them. And I think they should be endowed with serial numbers that will give you hard identification if you recover one in an illegitimate situation.

CHAIRMAN ERICKSON: You have suggested that you carry an inventory of some of these devices that are complete except for certain parts?

MR. HOLCOMB: That is correct.

CHAIRMAN ERICKSON: If that device was sold without that part, it wouldn't be a violation of the law as you understand it; is that correct?

MR. HOLCOMB: If it were sold without the parts?

CHAIRMAN ERICKSON: If it were sold without that part that was necessary to finalize the machine as an electronic surveillance device within the definition of Section 2512?

MR. HOLCOMB: Well, I don't know. I have never thought of it that way because I have never thought of selling one incomplete.

CHAIRMAN ERICKSON: You have never sold one that was incomplete?

MR. HOLCOMB: Never, ever. It would be extremely difficult for someone who was not one of our own in-house people either in the lab or in production to complete that device.

I think I probably could hand incompleting units to probably a hundred good technicians on the outside and they still couldn't complete it.

CHAIRMAN ERICKSON: Let me put it this way: Suppose you were to sell one of these devices that was complete with all but one part and were to make the other part available separately, so that it would be possible for the person to add this part, put Part A on Part B and the device will be complete.

MR. HOLCOMB: I think this would be absolutely an illegal act under the law and I think the intent of the law—

CHAIRMAN ERICKSON: But this could be done?

MR. HOLCOMB: This could be done. I don't know of anybody today who does this. And of course we certainly do not. As a matter of fact, when we sell something we want to recheck it and check it and check it again and we want to know it works just precisely how it should work before it goes out the door.

CHAIRMAN ERICKSON: I might ask you this. Since 1968 have there been material changes in the state of the art when it comes to electronic surveillance and bugging devices?

MR. HOLCOMB: Mr. Chairman, that is a difficult question. There have been material changes. But the changes in the devices used in 1968 and today are really not that different.

CHAIRMAN ERICKSON: Is the nomenclature different in so far as it relates to the devices and to the use of these particular items?

MR. HOLCOMB: Oh, the nomenclature has changed dramatically.

Prior to the law, for instance, an infinity transmitter, the harmonica bug, whatever you want to call it, was a surreptitious device, never intended for any other purpose. It was primarily sold and it was advertised for the man to put in his own house so if he was away from home or traveling on a trip he could call, and the phone did not ring but this let him know what was going on in the house.

It was sold in New York for this purpose for years. There was never any other purpose for which it was intended or designed.

Today it is on the market as an alarm system specifically for the purpose of someone calling their house or calling their place of business to determine if a burglary is in progress.

This is a pure farce. It is just not the case. The person who buys infinity transmitters buys them for one thing, and that is as an intercept device. It has always been that way.

CHAIRMAN ERICKSON: Mr. Morrissey, would you answer that question in the same way?

MR. MORRISSEY: In part, but there is a big exception that I think we should point out—the chilling effect that this law has on other related industries.

The statement was made that there should be total control of all wireless microphones. I think that is impractical and it is unnecessary. You are going to require the broadcast industry to go and categorize their equipment as surveillance equipment and suddenly they are tagged with the posses-

sion of identified surveillance equipment. The stage studios would have to do the same thing.

You are suddenly marking a product with a label that does not necessarily apply to it and I think it raises serious questions on free trade and as to what is its primary purpose.

Another point, though, in relation to the harmonica bug type of device is another type of device which was referred to as a talk-through circuit, which was tied in to burglar alarm systems.

And this operated so that whenever a premise was intruded it would alert a central security station with a light that an intrusion took place, and a talk-through circuit could be activated to tune in to the premise to determine how many intruders were there in order to know how many officers to dispatch, or the size of the activity, or if there was really any activity or false alarm.

But the wording here has caused a number of manufacturers to wonder whether or not they can legally incorporate this.

So it is spreading out into other fields and leaving a hanging question mark on it.

CHAIRMAN ERICKSON: Mr. Bower, would you add anything to the questions that I have just propounded?

MR. BOWER: I think not, Mr. Erickson, in view of the fact the discussion has centered around wired equipment. It is outside our sphere of activity.

CHAIRMAN ERICKSON: I would ask if your answers would be the same as Mr. Holcomb's and Mr. Morrissey's that in all probability this Act could be clarified, not only from the standpoint of the manufacturer but to make the Act more meaningful?

MR. BOWER: I don't think there is any question but that some clarifying phrases would be beneficial to all facets of the law enforcement community.

As I mentioned in my opening statement, the words "primarily useful" are very difficult to deal with along with definitions of lawful use.

CHAIRMAN ERICKSON: In your opinion is the literature that is available on this subject such that the trained radio repairman could acquire parts to build some of these devices without much difficulty?

MR. BOWER: I concur with Mr. Holcomb in that in most of the areas, particularly in the more complex devices, an average radio technician, as you have just described, would have considerable difficulty making a successful device without adequate training.

There are a lot of areas where adjustments are extremely critical and performance is very closely controlled where an average radio repairman—and that alone is a pretty difficult thing to identi-

fy—would have difficulty making a successful device from parts.

CHAIRMAN ERICKSON: Thank you.
Congressman Butler.

MR. BUTLER: Mr. Chairman, I have no questions. I think the staff has done a very fine job of putting this on.

CHAIRMAN ERICKSON: Thank you.
Chief Andersen.

CHIEF ANDERSEN: Mr. Bower, you talked earlier and one of the comments you made was on the fact of possibly licensing the receiver of the equipment or the user. You keep using the term "law enforcement agency."

Do you have any definition of law enforcement agency?

MR. BOWER: Yes, I do. My definition is the same as the statute, namely a political subdivision of the state or United States agency. In my view law enforcement agencies are government agencies.

CHIEF ANDERSEN: But just government agencies in the very broad sense?

MR. BOWER: I would say yes.

CHIEF ANDERSEN: What I am getting at is: In the Federal Register of May 20 they had the definition of criminal justice law enforcement concerning criminal records and one example they used was the Department of Agriculture which is classified as a subdivision of a law enforcement agency.

I am asking you if you had any problems with agencies which do not appear on their face to be law enforcement agencies?

MR. BOWER: That could be very deceiving, Chief Andersen. I would anticipate the Department of Agriculture would very definitely have law enforcement responsibilities in the area of conservation of natural resources, endangered species and areas of this sort. At least in many states in the East conservation departments within the state organization very definitely have enforcement responsibilities and as such would qualify under my definition.

CHIEF ANDERSEN: So you go back basically to the whole unit of government, if in fact it is a government letterhead concept?

MR. BOWER: And an enforcement agency. If they have laws to enforce, they definitely qualify under my definition.

CHIEF ANDERSEN: In licensing of users, do you think the burden should be on the government to define that rather than the manufacturer?

MR. BOWER: Yes, I do. Again, I think the statute as it stands defines the users adequately for my needs.

And I anticipate that Bell & Howell will always focus our activities in the law enforcement area rather than in a more broad area. So for that reason

I think that the definition is adequate as the statute is written, in terms of qualified users.

CHIEF ANDERSEN: One more question. On licensing a manufacturer which has been touched on pretty heavily here, do you think it is possible to license a manufacturer by individual units of production, or do you feel that the licensing should be of a manufacturer as an integrity business concept under some type of inspection system for what they actually are producing?

Do you think it is possible to define particular pieces of equipment that would come under a license? Is that possible in this technical world?

MR. BOWER: Yes, I think it is possible—perhaps not to reach perfection in this area but certainly an improvement can be made over present nomenclature. And I referred before to the words "primarily useful."

It would seem to me that some words that have been referred to earlier such as "body transmitters" and "wireless microphones"—it might be possible to even cite particular configurations without naming manufacturers that would properly define licensable, if you will, material or licensable manufacturers or divisions.

How each manufacturer would be treated would obviously be the responsibility of the licensing body, whether or not to license the entire corporation, for example, or an operating division or even an individual plant.

CHIEF ANDERSEN: Thank you. No more questions.

CHAIRMAN ERICKSON: Thank you, Chief.
Judge Shientag.

MS. SHIENTAG: Thank you, Mr. Chairman.

Mr. Morrissey, you object to licensing as an unnecessary method of controlling this field?

MR. MORRISSEY: Yes, I do.

MS. SHIENTAG: Had you given any thought as to whether a new agency specifically dealing with data banks and digital transmission and this whole area might be useful? Would that serve the purpose of controlling this?

MR. MORRISSEY: Yes, I think that is mandatory now at this time, the reason being that since 1968 the technical advancements and changes have brought about a whole new definition of what is electronic surveillance.

Now you could, with a portable computer terminal, dial in and drain a computer bank and you would not be intercepting any conversation.

MS. SHIENTAG: Isn't it alleged that something like that happened with regard to Equity Funding?

MR. MORRISSEY: Yes.

MS. SHIENTAG: And all kinds of industrial espionage can go on without this particular Act

properly protecting the corporations that might be spied upon?

MR. MORRISSEY: Yes. And the point you raised I think can be elaborated on to this extent.

Those individuals that are serious about pursuing criminal activity using electronics as a means of intelligence-gathering can get around the loopholes of this law, can see the vagueness of the wording, and if we don't more clearly define what it is we are going after, then we will eliminate the pettiness of the activity, but we will not get at the real core.

MS. SHIENTAG: And the penalty here is rather severe, five years imprisonment and/or \$10,000 fine for each offense.

MR. MORRISSEY: Yes, but I would point out that this law has never been taken to the Supreme Court and there have been cases where it could have been taken up to the Supreme Court, and it is the feeling of some that it was not done so by the Justice Department for fear that the whole law might be struck on the grounds of over-breadth and vagueness.

MS. SHIENTAG: You mean with regard to this section, 2512?

MR. MORRISSEY: Yes.

MS. SHIENTAG: And that section also provides in part for confiscation of the devices.

Now that, too, is an economic loss to a manufacturer when he acts at his peril without the knowledge of what the parameters of the offense are.

MR. MORRISSEY: More to the manufacturer, yes. But if we are going after the activity that uses this device, it is not a big loss in an individual sense.

Let's say, for example, equipment is sold from the manufacturer to a bona fide law enforcement agency. There is a large turnover in the agencies. Let's say, through this, some equipment goes unaccounted for and in some manner finds its way on the streets.

MS. SHIENTAG: But the Act does prohibit the manufacture, assembly, possession or selling of any electronic equipment, with the penalty of confiscation.

MR. MORRISSEY: Yes, that is right.

MS. SHIENTAG: That is what the language of 2512 now provides.

MR. MORRISSEY: Yes.

MS. SHIENTAG: Isn't it possible, were a manufacturer convicted, that that would put him out of business? He couldn't deal in these devices if he had a felony conviction?

MR. MORRISSEY: Yes, that is correct. I agree with you.

MS. SHIENTAG: And the officer of the corporation, if he were involved and personally prosecuted,

would have to retire from that business and forget all his knowledge and experience there; isn't that true?

MR. MORRISSEY: Yes.

MS. SHIENTAG: Now, I come from New York and I see that your literature, which we have had the benefit of having, states that: "B.R. Fox history dates back to 1955 where, in a small town 60 miles north of New York City—Holmes, New York—Bernard B. Spindel worked out of his two-story laboratory which nested in a rural setting in the foothills of the Berkshire Mountains."

That is very beautiful.

But I remember Bernard Spindel being involved in a conviction in connection with City Hall, some surreptitious wiretapping he did of City Hall some years ago.

MR. MORRISSEY: Yes, that is correct.

MS. SHIENTAG: And I don't recall what mayor it was but it was considered a very serious offense and I believe he was imprisoned. Am I correct?

MR. MORRISSEY: Yes, you are.

MS. SHIENTAG: That didn't prevent your company from continuing in this line of business, did it?

MR. MORRISSEY: Let me explain that to avoid any wrongful inferences. Mr. Spindel died in 1971. He was one of the foremost notorious individuals in this field prior to 1968. And it was this type of activity in the Fifties and the early Sixties that led to the enactment of the '68 law.

MS. SHIENTAG: But his was a private enterprise. It wasn't under the auspices of the police department in any way?

MR. MORRISSEY: That is correct. This was prior to 1968.

MS. SHIENTAG: So it was always illegal, even if there were wiretapping in New York, which had been authorized.

MR. MORRISSEY: Now, this was before the federal law was enacted in 1968.

MS. SHIENTAG: Yes. But there was a New York State law at that time which permitted police officers to do this and that was struck down. We have heard testimony about it today.

MR. MORRISSEY: Yes. You are not implying an association of mine with Mr. Spindel.

MS. SHIENTAG: An association? I am talking about your literature which sets forth his name.

MR. MORRISSEY: Okay; yes.

MS. SHIENTAG: And the point I am making is that that has not prevented you from continuing in business—his conviction and his association with your firm.

MR. MORRISSEY: No, there were two separate operations, but you are right; no.

[Relevant material follows.]

2701 Fairview Drive
Alexandria, Va. 22306

July 31, 1975

General Hodson, Executive Director
National Commission for Review of Federal
and State Laws Relating to Wiretapping and
Electronic Surveillance
Washington, D.C.

Dear Sir:

I am taking the liberty of writing to you regarding certain portions of your hearings on Wiretapping and Eavesdropping conducted by Mike Hershman, specifically in reference to pages 64 through 66 of the transcript, in which certain factual inaccuracies are stated, and certain incorrect inferences result. I sincerely hope that you will include these corrections (noted below) as part of your report—and accept them in the spirit in which they are intended: to shed further light on a tangled piece of legislation and to correct any wrongful impressions.

I also wish to state the following comments are limited to pages 64 through 66 of the transcript as I had only an opportunity to spend a lunch hour in your offices going over (as quickly as possible) pertinent pieces of testimony. I would appreciate a copy of the testimony for my review if one can be spared.

Specifically:

p. 64—Ms. Shientag—Line 11 through 14; Lines 16 through 23: Mr. Bernard Spindel was NEVER an officer of B.R. Fox Company, Inc. The company was incorporated in New York State in the fall of 1969, with three officers: Barbara R. Fox (Spindel); Herbert R. Burris; and Richard J. Butterfield. Mr. Michael J. Morrissey did not become an officer of the corporation until July of 1971—and in actual fact, did *very little work with Mr. Spindel or for the corporation prior to that date.*

Mr. Spindel was convicted in June, 1969, of "CONSPIRACY TO GIVE TECHNICAL ADVICE ON A WIRETAP" based on a three-count indictment in connection with the Huntington Hartford divorce case**—*he was never in any way involved in a wiretap on New York City Hall, nor was he ever convicted of such a charge.*

From the time of Mr. Spindel's conviction (above) in June of 1969, he ceased ANY AND ALL association with B.R. Fox Company. Upon his parole from prison in 1970 (August), he remained disassociated from B.R. Fox Company, Inc., as he otherwise would have been violating the terms of his parole.

All of the technical devices and designs and knowledge handed down to B.R. Fox Company by Mr. Spindel were PRIOR to 1969—and it is actually a tribute to the genius of the man that devices which were designed so far back in electronic history are VALUABLE today and are current, despite the rapidly changing world of electronic engineering. Mr. Morrissey, on the other hand, NEVER IMPROVED ON MR. SPINDEL'S DESIGNS IN ALL OF THE TIME HE WAS ASSOCIATED WITH THE COMPANY.

There is much else I feel could be added to your report to give it both substance and validity, and I mentioned to Mike Hershman a long time ago that I would be more than glad to cooperate with your Commission. Not only that, it was I who gave Mr. Hershman all of the files involving actual orders from police departments, the names of the departments involved in the B.R. Fox training school, etc. Mr. Morrissey, in fact, put a number of stumbling blocks in the path of compliance with your Commission's subpoena by removing all of the files and filing cabinets from their legal business location at 2701 Fairview Drive, Alexandria (the address of the corporation), the day the subpoena was received.

I will be more than happy to review and comment on the balance of the draft report if you so desire, and if I may have a

copy of that report on loan for a period of at least ten days. Additionally, I am enclosing for your information, a letter sent by Mr. Spindel to the Congress (both houses) at the time of the consideration of Title III. I believe it will prove helpful for your writing of your final report and recommendations. I would suggest also that you check the Long Committee testimony of Mr. Spindel's because that testimony is still pertinent to the consideration of any wiretapping or eavesdropping legislation.

I have changed my place of employment and am now working at the Department of Agriculture. If you wish to reach me, or if Mike Hershman wishes to reach me, I can be called at 447-3831 or 447-3832.

Thank you.
Sincerely,

[Signed] BARBARA FOX SPINDEL
President
B. R. FOX COMPANY, INC.
(presently being dissolved)

Enclosure

BERNARD B. SPINDEL

LUDINGTONVILLE ROAD, HOLMES, N.Y. 12531
914-878-6846, 6136

ELECTRONIC SECURITY CONSULTANT

May 16, 1968

Dear Senator:

IN REGARD TO BILL S-917, TITLE III

I have just read the printed version, dated April 29, 1968, of the above-mentioned bill, and I am very disturbed by the inadequacies, contradictions and detrimental effects that this bill would have on LAW ENFORCEMENT; which is directly contrary to the legislative intent of the total bill.

I am in complete agreement with the protection of privacy, and with the reduction of crime, by whatever means necessary. To save a lengthy report, I will itemize the points which should be amended and incorporated into the bill now proposed, and state briefly my reasons for such recommendations:

1. More than 90% of all Research and Development in the field of (No. a) Electronic Eavesdropping, and (No. b) its counter measures and detection and prevention, have been through the efforts of private enterprise and individuals. Obviously (No. b) cannot possibly be accomplished without experimental work in (No. a).

Electronic sophistication in this field necessitates constant Research and Development and under the provisions of this bill, there is absolutely no provision for serious-minded scientists, experimenters, or inventors, to possess the equipment necessary for such experimentation. In the long term, therefore, even our very *National Security will be adversely affected.*

2. The S-917, Title III, Section 2511 (2c) authorizes an individual to record conversations to which he is a party, or where the prior authorization exists from ONE of the parties involved in a particular conversation; the police, by regulated Court authorization, within this legislation, would have the right to record telephonic and oral communication . . . HOWEVER THIS BILL (SECTION 2511) PROHIBITS THE MANUFACTURE, DISTRIBUTION, POSSESSION, ADVERTISING, ETC. of these devices. Therefore, the question becomes "how are the police departments (or the private individual recording his OWN conversations) supposed to obtain these devices if no one is allowed to manufacture them or their components". This would also prevent legitimate police suppliers and force legitimate dealers for counter industrial espionage, from possessing, obtaining, manufacturing, using or advertising, any of the necessary paraphernalia.

There are certainly other legitimate uses which would further aid in crime prevention, detection and apprehension. I am now

**See *The People of the State of New York vs. George Varris, John Connors, Richard Rutherford and Bernard Spindel No. 4817 1/2—1966*

personally involved in the Research and Development of a Radar Type Intrusion Alarm which would be wired directly to police communication headquarters throughout the country, and I have developed a new "talk/through" circuit which, beyond the normal furnishing of an alarm caused by an intruder, would enable the policeman in the central office to determine the validity of the alarm, whether "false" or otherwise, and would tell him approximately how many burglars are on the scene and how many cars to dispatch to apprehend the burglars. In addition, the proposed "listen talk/through." circuit for the burglar alarm would automatically record the voices of the intruders, who could then later be identified by "voice print." However, under the terms of Title III, S-917, this would be illegal without a court order for each and every intrusion.

Under Bill S-917, we would have to stop all research and development and in effect, we will be defeating the very purpose intended by the "Safe Streets Bill"; that of preventing crime and apprehending the criminal.

There are no exceptions in this bill, and at best it is ill-conceived, and should be amended to include the above, or else tabled in its present form, until more time and effort can be expended in the drafting of a more intelligent and definitive bill. From a technical point of view, the bill at present does not begin to cover the possibilities that exist on the drawing board at present, including such things as jumping the circuitry on a video phone to permit the seeing of activities in a room even when the phone is hung up, and will in effect be adverse to the protection of our citizenry and to our NATIONAL DEFENSE EFFORTS. I urgently recommend the amendment or defeat outright of Title III of S-917, and will be more than glad to give my technical assistance you may require.

Very truly yours,

[Signed] BERNARD B. SPINDEL

P.S. I have just released my book entitled "The Ominous Ear", published by Award House/Universal Publishing Corporation, and distributed by Crown Distribution. The book covers this particular subject at great length.

MS. SHIENTAG: Now, with regard to licensing, Mr. Holcomb, I read your statement and I found it very useful. But what concerns me is this: How would you license the equipment that is presently on the market such as telephone answering devices and matters like that? Do you think you could ban all that material?

MR. HOLCOMB: No, Ma'am. I don't believe that you can go back in the game after you have already lost and pick up all the marbles. I think there are going to be some abuses by virtue of the devices that have been sold in the past—no question about this. And I don't imply that everything should be licensed.

I feel that definitions—and I have wrestled with this for weeks and weeks with attorneys—I feel that definitions can be adequate to define the large majority.

Now, in some cases this has to be done in a little bit of a unique manner, a manner different than you might ordinarily have definitions. But, nevertheless, I think that the control of these things in the future is mandatory if you are going to stop the problem. Because the problem is not primarily

with the police officer or the law enforcement agency that can openly purchase equipment. The problem in the majority of cases is with individuals, private persons—look at the Watergate situation. This is the classic that will end up being the classic of all times.

But here again the law fails in that—look at the penalties put on the people who pleaded guilty or were convicted on this. They got a slap on the wrist for a few months and walked out of the door.

MS. SHIENTAG: Thank you, Mr. Holcomb. We are concerned with the licensing suggestion you made. I don't think that would relate to Watergate.

Do you think that a new agency specifically designed to deal with all the advances in the state of the art—even before 1968 but certainly since then—might be a useful alternative to the licensing proposal that you expect to send us?

MR. HOLCOMB: No, Ma'am. I think we have too many agencies now. I would much rather see an agency that has a track record and a performance behind them, which I think ATF has.

MS. SHIENTAG: ATF and the Treasury?

MR. HOLCOMB: ATF has a track record and if you look at what they have been able to do in the automatic weapons field—and there are so many similarities—I think they could well manage under a law that would be definitive.

MS. SHIENTAG: Thank you, Mr. Holcomb.

CHAIRMAN ERICKSON: Thank you, Judge.

Professor Blakey.

PROFESSOR BLAKEY: Mr. Chairman, in light of the late hour, I don't think I will address questions to any of the witnesses. I would, however, like to express a general feeling I have, having listened to what they have had to say.

Frankly, I am troubled by responsible manufacturers engaging in training of officers who have no legitimate need for the activity that they are trained in. It seems to me that borders on irresponsibility.

I am very troubled by what I see as a "hear no evil, speak no evil" attitude about the sale of devices primarily useful for surreptitious interception of communications to police officers in states that have no authorizing statutes.

You have all testified that you make an effort to determine whether people are police officers and I think that is a move in the right direction, but it seems to me you could make some reasonable effort to determine what the laws of the states are; and that if there is no law whatsoever, in a particular state that is not too difficult to determine.

And frankly, I am not impressed when you suggest that devices designed for surreptitious surveillance may also be used for one-party-consent surveillance. I think that is stretching it a bit. When I

look at some of the kind of devices some or all of you have been selling to states, no reasonable man would buy that device with an idea of using it for one-party interception situations. And it seems to me that that fact is transparent.

Finally, I would hope that as a result of these hearings you would go home and speak with your lawyers and reconsider your policy.

It seems to me if you are not violating the law you are treading on the outer edges extremely closely.

CHAIRMAN ERICKSON: Thank you, Professor Blakey.

I might say, gentlemen, that the Commission is deeply indebted to you.

Mr. Hershman, you have a closing statement to make and upon that statement being made we will take a brief recess and then go immediately into the display of electronic surveillance equipment and take Mr. Bragan's testimony somewhat later.

Mr. Hershman.

MR. HERSHMAN: Just for the purpose of clarification before the Commission, I would like to add that Mr. Morrissey is no longer connected with B.R. Fox, a company which is now defunct and has been out of business since 1974. Mr. Morrissey has aided the Commission immeasurably and has provided to us records of the sales of B.R. Fox when he was affiliated with it.

I would add that we have found no abuses in the method of operating B.R. Fox when he was managing it.

Thank you.

CHAIRMAN ERICKSON: Gentlemen, I am again very grateful for what you have done for the Commission. I hope that the testimony that you have offered will result in the improvement of the law relating to electronic surveillance and wire-tapping.

Thank you again.

We will be in recess for five minutes.

[Whereupon, a short recess was taken.]

CHAIRMAN ERICKSON: Ladies and gentlemen, may we reconvene?

At this time we will present a demonstration and display of electronic surveillance equipment.

The presentation will be by two gentlemen who have been working with the Commission.

Mr. VanDewerker is General Manager, Systems Division, Ashby & Associates, and is currently conducting a state of the art study of electronic surveillance for the Commission.

[Material on display equipment follows.]

DESCRIPTION OF ELECTRONIC SURVEILLANCE EQUIPMENT TO BE DISPLAYED

Tri-Tap Transmitter - A room transmitter built into a tri-tap plug which can be plugged into any AC outlet. This transmitter is activated by the AC line and voices up to thirty feet away can be transmitted to a receiver up to a distance of five hundred feet.

Drop-in Telephone Mouthpiece Transmitter - Replaces the standard mouthpiece microphone, and will transmit both sides of the telephone conversation. The device is self-powered and can be installed in 5 seconds.

Infinity Transmitter (Harmonica Bug) - The device is secreted in the base of a telephone using a two wire connection. Thereafter, subject's phone can be dialed and the device activated by a pocket-sized tone generator. The telephone will not ring and the tone will connect a high gain microphone amplifier to the telephone line, thereby allowing audio surveillance of all room sounds within a radius of 30 feet of subject's phone. The device is deactivated by hanging up the telephone from which the subject's number was dialed.

Automatic Telephone Line Intercept - A wired telephone intercept device which allows for interception of room as well as telephone conversations. Requires modification of telephone instrument and is installed anywhere between the telephone and central office.

Light Beam Transmitter - A narrow beam invisible light source which converts sound energy to an optical signal which is then transmitted to a suitably located detector. Generally, the detector (receiver) must be located in line of sight with the transmitter. The device is powered by an AC line.

Carrier Current Transmitter - A miniature transmitter, powered by an AC power line, which converts sound energy to electrical energy. This energy is passed along the power line to a receiver. Picks up conversations at 50 feet and transmits them up to great distances.

Vehicle Tailing System - An intermittent pulse transmitter which is designed for magnetic attachment to a vehicle. This device transmits a signal which allows for tailing the vehicle. Not designed for interception of oral or wire communications.

Sub-Miniature Microphone and Control Box - An ultra-miniature microphone with integrated preamplifier which monitors room conversations and transmits them using existing electrical or telephone lines. Operative for distances up to 25 miles, the device is controlled remotely and can be deactivated from the listening end.

Miniature Drop Transmitter - A miniature transmitter designed to be dropped in a room, placed in furniture, or stuck on the wall. Powered by a 9-volt battery, the transmitter will give approximately 18 hours of continuous transmission.

Telephone Slave Unit - Provides monitoring of a telephone line, or a room bug, from any remote location by dialing a number (line 1) to which one side of the slave is connected. The slave switches the caller from line 1 to whatever is connected to the other side of the slave, usually the subject's telephone line (line 2). This allows for the monitoring of all conversations on line 2. Long distance unattended coverage can be obtained by using a voice actuated circuit.

Remote Tone Activation Kit - Provides for remote activation of transmitters.

The above equipment has been furnished by:
Bell & Howell Communications Company
Martin Kaiser, Inc.
Michael J. Morrissey
Security Specialists, Inc.

Aspirin Tablet Transmitter - This particular transmitter is a self-excited FM transmitter tunable over the frequency range of 75-150MHz. It is practical to include a power amplifier in the same package with different fabrication techniques.

The power output is approximately 0.3 milliwatts with a 1.35 volt battery and has a range of 2-3 blocks. Stacking a second cell in series will give a power output of approximately 2 milliwatts and a range of about 1/2 mile.

The transmitter was originally designed to be ingestible for the tracking of people, together with an ingestible receiver, for purposes of foiling kidnappers.

A separate RF package also accompanies the operable unit to show the physical size. Components are extremely tiny and well fabricated. One of the internal inductors is wound with 15 turns of No. 54 wire (.0007 inch diameter, about 1/5 the diameter of a human hair. The toroidal core is about the size of the head of a straight pin.) It will be noticed that a miniscule hole exists through the package. This is the hole through which a plastic broom-straw can be used to move an internal core for adjusting the operating carrier frequency.

Postage Stamp Transmitter - This particular transmitter is a multipurpose device. It can be used over the frequency range of 85-140MHz. Its power output can be adjusted from 0.5 Milliwatts to 25 milliwatts depending upon the battery voltage applied, and the type of modulation impressed.

It will be noticed that a pair of the pins are shorted. In this condition, the unit is self-excited. Removal of the short and the substitution of a crystal results in a crystal controlled transmitter. Again, two small holes can be noticed through the case. The first is for the tuning of the oscillator, and the second is for tuning the power amplifier to resonance. The remaining pins are for the microphone attachment, power connection, and antenna.

This unit is unique in that it can be used for conventional continuous carrier FM modulation, or pulsed with two microsecond wide pulses for data transmission.

Tracking Transmitter - Designed primarily for tracking, this transmitter is rather unique in that it will function for several months from a small battery pack, yet generates an output power in excess of one watt. Designed for minimum power consumption, the unit is pulse modulated.

The unit is comprised of two assemblies, the smaller containing all of the RF circuitry, and the larger containing the modulator.

Several terminals are visible on the side of the modulator, allowing a selection of the number of pulses in a pulse group, and also allowing a setting of the time interval between pulse groups e.g. you can select one, two, or three pulses in a group, and vary the time interval between groups from three seconds to thirteen seconds.

The composite transmitter is modularized to allow substitution of different types of modulators. Thus, it is possible by substituting a coded modulator, to endow the transmitter with an equivalent power output in excess of 2000 watts.

The unit is crystal controlled.

Microwave Transmitter - This transmitter is a brassboard experimental transmitter consisting of an oscillator and power amplifier. Its carrier frequency is 1420 MHz. Power output is 100 milliwatts peak power. Antenna length is 5 inches. The unit is pulse modulated with 1 microsecond pulse width. Applicable to the transmission of data, or voice modulated.

CHAIRMAN ERICKSON: Mr. Fahy has been working as a consultant for the Commission in the southern states since 1974.

[Whereupon, John S. VanDewerker and James T. Fahy were duly sworn by the Chairman.]

CHAIRMAN ERICKSON: At this time I call upon Mr. Hershman.

**TESTIMONY OF JAMES T. FAHY,
CONSULTANT, NATIONAL WIRETAP
COMMISSION; AND JOHN S.
VANDEWERKER, GENERAL
MANAGER, SYSTEMS DIVISION,
ASHBY & ASSOCIATES**

MR. HERSHMAN: Mr. Fahy, I wonder if you would lead off with the first piece of equipment and explain the nomenclature and how it operates.

MR. FAHY: This (indicating) is what is commonly referred to as a drop-in transmitter. It is the shape, size, and color of the one that is in the mouthpiece of the telephone. In actual operation the transmitter of the telephone is taken out and replaced with the drop-in transmitter which will broadcast both sides of the conversation being conducted on the telephone.

I would like to demonstrate this to you.

MR. HERSHMAN: Would you show us please, Mr. Fahy, the similarity between the drop-in transmitter and the telephone mouthpiece.

MR. FAHY: This (indicating) is the actual mouthpiece of the telephone, and this (indicating) is the drop-in transmitter.

MR. HERSHMAN: Will you hold that up so the Commission can see it, Mr. Fahy.

MR. FAHY: That (indicating) is the drop-in transmitter and this (indicating) is the one from the telephone.

MR. HERSHMAN: So there is actually little physical difference between the two; is that correct?

MR. FAHY: That is correct. This ordinarily takes less than five minutes to implant into the telephone.

We have set up over there a portable radio receiver which will be able to pick up this transmission.

I am going to dial the local weather in the Washington area.

And at the same time I can be speaking into the telephone and both sides of the conversation will be broadcast through the air and received at a remote location.

MR. HERSHMAN: So if this device is implanted in a telephone, as soon as the individual picks up the phone, begins dialing and has his conversation, both sides of the conversation are recorded?

MR. FAHY: Yes, sir, that is correct.

MR. HERSHMAN: And is that device sending a radio frequency signal?

MR. FAHY: It is a radio frequency signal and the power supply is supplied by the telephone line, itself. There is no battery installed so the device will function almost indefinitely.

MR. HERSHMAN: So there is no need to return for maintenance of the device; is that correct?

MR. FAHY: No, sir, once it is installed, it works almost indefinitely.

MR. HERSHMAN: To what distance will that transmit?

MR. FAHY: In this configuration there is no transmitting antenna so the range is quite limited. I would say a block to a block and a half away.

MR. HERSHMAN: Would you consider that, Mr. Fahy, to be a sophisticated device among those which are today commercially available?

MR. FAHY: No, I wouldn't consider it sophisticated, sir.

MR. HERSHMAN: Is that more apt to be used in the private sector by individuals engaging in domestic espionage or industrial espionage?

MR. FAHY: Yes, I believe that would be the prime market for it.

MR. HERSHMAN: Do you have any idea what something like that would cost, Mr. Fahy?

MR. FAHY: They range approximately from \$200 to \$500, depending on the manufacturer.

MR. HERSHMAN: And would it be difficult with the proper components for a non-technical individual to build one of those (indicating)?

MR. FAHY: For a non-technical individual? No, he would have quite a problem putting it together. It is miniature circuitry and must be confined within the same area the original transmitter fits into.

MR. HERSHMAN: And as we can all see, the installation time is relatively fast.

MR. FAHY: The installation time would be a matter of a minute or two.

MR. HERSHMAN: How difficult would that be to detect using counter-measure methods?

MR. FAHY: It can be readily detected.

MR. HERSHMAN: Can it be detected by visual inspection?

MR. FAHY: Yes, it can.

MR. HERSHMAN: Can you tell us what some of the characteristics are which distinguish it from the ordinary mouthpiece?

MR. FAHY: Primarily—I am having a little problem with it already in that it is difficult to get out of the case once it has been implanted. The original transmitter drops right out. This one sometimes has to be pried out.

On the bottom of the drop-in device, you will notice it is quite a bit thicker than the original transmitter (indicating).

On the surface they are very similar but on the back side there is quite a difference between them (indicating).

MR. HERSHMAN: Mr. Fahy, you have quite a number of years of experience, being a retired New York City police officer. Tell me how long have these devices been available in the United States?

MR. FAHY: To the best of my knowledge, this drop-in device has been available for at least ten years.

MR. HERSHMAN: Thank you.

Would you go to the next device, please.

MR. FAHY: On the next device we do have a chart made up here, if you will just give me a moment to get the proper one out.

The first device that we have charted here is what is referred to as a Slave Unit.

MR. HERSHMAN: Mr. Fahy, could you swing your chart this way a little bit so Chief Andersen can see it.

MR. FAHY: Can you all see that?

MR. HERSHMAN: Yes, thank you.

MR. FAHY: This is the actual device (indicating). As I mentioned, it is referred to as a Slave Unit. Its purpose is to connect one telephone line to another telephone line.

On our chart here we have displayed the subject telephone or the target telephone, the green line (indicating) being the existing telephone line running from the central office up to the subscriber's home.

This (indicating) is what is called a terminal box. Here (indicating) are what are called binding posts that the actual telephone lines are connected to.

For the installation of the Slave Unit, it is necessary to have either a leased or friendly telephone line, said line being used to interrogate the subject's line.

The Slave Unit is attached between the subject's line and the leased or friendly line.

This brings us up to the termination of the leased or friendly line (indicating), where the listening post is established.

From anywhere in the country or possibly from anywhere in the world, what is required for the man to eavesdrop on this phone is to call the number assigned to this leased or friendly line. Upon calling, the Slave Unit automatically switches over all of the conversations, be they room or telephone, along the leased line and back to this phone which can be placed anywhere in the country or the world. And of course recording is possible at that location.

MR. HERSHMAN: This device has not only the capability of recording telephone conversations but room conversations as well?

MR. FAHY: Yes. If a voice pick-up device had been implanted in the room it is definitely possible to monitor and record the conversation.

MR. HERSHMAN: Where would this be attached, the remote Slave Unit?

MR. FAHY: It must be attached somewhere in the terminal box so it can be attached to the leased or friendly line, and also to the subject's line at this location.

MR. HERSHMAN: And this means you can have a listening post virtually any place in the country; is that correct?

MR. FAHY: That is correct.

MR. HERSHMAN: And once you dial the subject's phone it opens up the circuits and enables you to monitor the conversations?

MR. FAHY: Yes. It can be done at random for a sampling of the conversation or it can be maintained continually.

MR. HERSHMAN: What does this device cost?

MR. FAHY: It starts at \$200, anywhere up to \$500, depending on sophistication.

MR. HERSHMAN: What is the length of installation time?

MR. FAHY: It would depend on how readily a leased or friendly line would be found in this area (indicating). The actual hook-up could be anywhere between two to five minutes.

MR. HERSHMAN: Would you need cooperation from the telephone company to install one of these devices?

MR. FAHY: Possibly with the obtaining of a leased line, yes.

MR. HERSHMAN: Would you tell us what a leased line is?

MR. FAHY: It is a line that is not used ordinarily in a cable and it is similar to an off-premise extension. The leased line is rented by the telephone company to the subscriber who usually pays a mileage charge on it, costing the user so much per mile.

MR. HERSHMAN: Is this a relatively sophisticated device, sir?

MR. FAHY: To some degree, yes, sir.

MR. HERSHMAN: Do you find it is more adaptable to use in law enforcement or in the private sector?

MR. FAHY: I would say it would be more adaptable in law enforcement.

MR. HERSHMAN: Mr. Fahy, if in fact you do connect your own line to the terminals, how do you determine what the pair and cable number is?

MR. FAHY: That requires some previous background in telephone work. You do have to know at this location where the termination of the existing telephone line is which serves the subject of the intercept.

MR. HERSHMAN: You can, however, determine the correct line, the pair and cable line without getting that information from the telephone company; is that correct?

MR. FAHY: Yes, sir.

MR. HERSHMAN: Can you tell us what the method of doing that is?

MR. FAHY: Yes, there are many ways to do it. If you have what is called a telephone company test set you would know the subject's number, because that is going to be your target. You would be aware of his number. If we enter this terminal box (indicating) or cross box, and went across the pairs in here (indicating), and rang that number to get what is called the busy back or dial the operator as a repairman and find what line we are coming up on, it would be quite easy to determine what pair in that box it was that we were interested in.

MR. HERSHMAN: If you didn't have that lineman's handset, is there another method of shorting the terminals to determine?

MR. FAHY: Yes, there is.

MR. HERSHMAN: And how does that work?

MR. FAHY: You would still have to know the number. You could get on another working line in the same cross box, dial the subject's number, and run rapidly down the terminals with a tool or a coin. Upon shorting the subject's terminals with the tool or coin a loud click would be heard in the test set earpiece.

MR. HERSHMAN: I see. And is there any difficulty in determining which terminal box the pair exists in?

MR. FAHY: Not to any degree. Ordinarily you would go possibly to the closest one in the proximity of the subject.

From there there is a great possibility, also, of going out to other locations, anywhere between the subject's line and the central office serving this area.

MR. HERSHMAN: In other words, that same pair has a multiple appearance at another location?

MR. FAHY: Yes, many have at least two or three appearances.

MR. HERSHMAN: So it is not necessary to make the connection within the building that the telephone is located in?

MR. FAHY: No, sir, it could be many blocks away.

MR. HERSHMAN: Mr. Fahy, does this device implant any interference on the line so the subject might become aware that he is being listened to?

MR. FAHY: No, sir, there is no interference placed on the line with the Slave Unit.

MR. HERSHMAN: How difficult is it to detect if you were looking for it?

MR. FAHY: It would be readily detectable with fairly sophisticated counter-measures.

MR. HERSHMAN: Would it be detectable by visual inspection?

MR. FAHY: If you could examine the entire interior of this box (indicating), yes. But it is possible due to its small size to be secreted behind a large cable or bundle of wires.

MR. HERSHMAN: Thank you.

Would you go on to the next piece of equipment, please.

MR. VANDEWERKER: The next device is the automatic telephone line intercept.

This particular system is used in conjunction with a modified telephone instrument, and requires access to the premises by the eavesdropper and some limited disassembly of the telephone.

Normally this includes just the removal of the telephone case and the installation of a small, readily available electronic component or the simple movement of a wire internal to the instrument.

What this does in effect is by-pass the hook switch contained within the instrument. This switch is activated when the button is depressed and the receiver is in the normal hung-up position.

Once this switch is by-passed, room audio can pass through the telephone out onto the telephone lines. To retrieve the audio signals requires access to the telephone pair in a manner similar to the device just described. This access may come at a terminal box or at the exterior of a building and does require the identification of the target pair of the telephone.

Once this pair is located, this particular piece of equipment is inserted in serial with the line, such that the eavesdropper can monitor the room conversation, yet, when an incoming telephone call comes in on these lines, the device will alert the eavesdropper and connect the incoming ring to the telephone instrument so there is not any alerting of the suspect.

MR. HERSHMAN: And, Mr. VanDewerker, what you are telling us, then, is that this device, once hooked up, will monitor all room conversations while the receiver is in the down position on the phone; is that correct?

MR. VANDEWERKER: Yes, sir, that is correct.

MR. HERSHMAN: What happens if the receiver is picked up?

MR. VANDEWERKER: If the compromise or the telephone modification is designed to exploit the talk pair of the telephone, that is, the normal pair which is used for the passage of telephone communications, then the eavesdropper might well be able to record and monitor the telephone conversation similar to the tap practices.

MR. HERSHMAN: Now, the piece of equipment that is necessary inside the telephone—does this look like any other piece of equipment inside your telephone?

MR. VANDEWERKER: The internal installation of a compromise component might appear in various forms. The simple movement of a wire, as in the case of a third-wire modification, would not be recognizable by the casual observer or even, in many cases, by the skilled observer.

However, some components might be so small, that is, the size of the head of a pin or a match head, that they could be easily concealed within the inner workings of the telephone instrument. They would not be readily apparent and frequently it is necessary to x-ray the instrument to determine if there has been a small device placed internal to the instrument.

The small device I am referring to could be anything from a diode or a small neon bulb or a silicone-controlled rectifier. These terms are all common to the lay technician and certainly readily available from radio-TV shops for a nominal cost, frequently less than \$1.

MR. HERSHMAN: How long would it take to install a device of this nature?

MR. VANDEWERKER: With some practice it might only require the matter of a few minutes to install this device.

However, without practice it might take quite a lengthy period of time. The installer does have to remove the cover from the telephone instrument and identify the proper wires. On a single-line instrument it is relatively simple and straightforward. However, in the complex multi-button telephones used frequently in business offices nowadays the cable bundle exiting has 50 wires which can give the combination of 1200 pairs. So the installer would have to have knowledge of the pair he wished to use, and knowledge of the internal system, before he made the installation. But once he had this it might still take less than five minutes for an installation.

MR. HERSHMAN: This device is powered by the current in the telephone system, sir?

MR. VANDEWERKER: This device at the option of the eavesdropper may or may not be powered by the telephone line current. This particular one displayed today (indicating) does not use telephone line current. It has a self-contained battery which will provide the current necessary to activate the telephone. Thus, the telephone company is not alerted by an unusual power drain from their system by the manipulated telephone.

MR. HERSHMAN: This passes the oral communications down the wire and it is picked off of the wire; is that correct, sir?

MR. VANDEWERKER: That is correct.

MR. HERSHMAN: How far a distance can you be from the subject's phone to receive these communications?

MR. VANDEWERKER: You are essentially only limited by the distance between the target phone and the first switching station or central office. In some cases it may be several miles between an instrument and a local switching station.

However, in a larger system where the central office is located, for example in New York City, many large companies share a central office, a localized office, and the installation would have to be made between that point and the telephone instrument, itself.

However, with the addition of a radio transmitter to the telephone line pair, the audio present on the telephone line pair might be transmitted to any distance whatsoever.

MR. HERSHMAN: Now, if this device is installed correctly, can you tell us what the quality of the audio received would be?

MR. VANDEWERKER: Yes. The quality is very excellent in most cases where the mouthpiece is used. I can quantify it somewhat. In normal use the telephone mouthpiece draws perhaps 50 milliamperes of current and a normal intercept of this type might draw only one-half or one-hundredth of that amount of current, yet the quality of audio produced is very good. The mouthpiece of the telephone has been refined and developed over the years to be rugged, reliable, and sensitive, and with that amount of current passing through this instrument this telephone could readily retrieve any audio present in this room today.

MR. HERSHMAN: And what does a device like this cost, Mr. VanDewerker, approximately?

MR. VANDEWERKER: The component or components required for the modification of the telephone might cost one or two dollars. The actual device for retrieving the audio amplifier, and perhaps an alerting light to indicate when there is an incoming ring, plus a throwswitch to allow the eavesdropper to connect an incoming call to the target telephone. In this way he would not alert any incoming callers or the target.

So, cumulating the cost of these components you might readily be expected to produce this system for less than \$50, if you were to design it and choose your own devices.

MR. HERSHMAN: Is this device more apt to be used in the private sector, would you say?

MR. VANDEWERKER: The modification of the telephone instrument is not widely known or understood by the private sector. It is understood to some extent by law enforcement organizations. The

private sector is somewhat confused by the term "bugging" of the telephone, and you see conflicts in the literature which describe a modified telephone as a bugged telephone, which also describes the implant of a mouthpiece transmitter.

This device (indicating), the mouthpiece transmitter, is an RF tap. The other is a room transmitter device. That is its primary purpose. However, as I said, if the talk pair is used, it also may double as a wiretap device.

MR. HERSHMAN: And how long would it take for an experienced countermeasure technician, a debugger, say, to discover this system?

MR. VANDEWERKER: This particular system on display today would be relatively easy to detect by a competent countermeasures expert.

Now, the difficulty arises when the eavesdropper is clever enough to use various voltage-actuated or switching devices, so discovering their presence requires a stimulating signal on the telephone line to activate the device.

MR. HERSHMAN: Thank you. Can we go on to the next device.

Before we leave that particular device, is it reasonable to assume that this device could normally be used for the monitoring of one-party consent conversations?

MR. VANDEWERKER: Not normally. I would guess in given situations where a telephone instrument might be installed in an area, it might be required as a cover device, for example, in a situation where two individuals were talking.

MR. HERSHMAN: Let me ask you this, Mr. VanDewerker: Are there better devices to use for one-party consent than this one?

MR. VANDEWERKER: Yes, there are.

MR. HERSHMAN: Would you pay that amount of money for a device like this in order to use it for consensual monitoring?

MR. VANDEWERKER: The amount of money involved in this type of penetration technique is actually very small and it might be a reason to use this technique as compared to perhaps some others.

MR. HERSHMAN: But if it was being purchased from a commercial manufacturer, would this compare in quality and effectiveness to your devices which are more designed for one-party consent monitoring?

MR. VANDEWERKER: No, sir, I think there are a number of technically less sophisticated ways that would be much more practical to install and use.

MR. HERSHMAN: So what you are saying is there is no doubt that this particular device—and I think we can safely say the Slave Unit, also—is primarily useful for the surreptitious interception of wire and oral communications?

MR. VANDEWERKER: Yes, sir.

MR. HERSHMAN: And would you say that it would be a wise use of funds by a police department to purchase this for use in one-party consent monitoring?

MR. VANDEWERKER: No, sir.

MR. HERSHMAN: Thank you.

Could we go on to the next device, please.

MR. FAHY: Our next device is called the harmonica bug or infinity transmitter.

The original devices made were activated by a small harmonica, a single-note harmonica, and that is where the name "harmonica bug" comes from.

This is, as you will notice, a small imported harmonica with a piece of tape around it with the exception of one of the notes. And that note is used for activation of the device.

If we refer to the chart over here (indicating) you will note there are two alligator clips coming out of the infinity transmitter. These clips are attached to the telephone line at any location within the premises. The telephone line goes into the central office. The phone will operate normally. It does take a little bit of current to operate the infinity transmitter. There may be a slight reduction in volume level, ordinarily not noticed by the target.

If we have our harmonica with a single note at any remote activation place, we can trigger the infinity transmitter on.

These are made in several configurations. One configuration will interrupt the ring, so should the infinity transmitter be located in the premises, the monitoring person calls that premise, activates the tone generator or the harmonica and the phone will not ring in the premises but it will automatically switch the infinity transmitter on, which brings back over the telephone lines all the room conversations going on in the area in which it is implanted.

We would like to give you a demonstration of this.

We have two instruments over here.

We only have a small table here but the distance between the two instruments can be infinite. They don't have to be in close proximity or be installed within the same central office location.

The device that we have here is the type that you must call to the other phone first, possibly as a wrong number call. When the phone is hung up on the far side, by applying this tone generator or harmonica to the mouthpiece of this telephone (indicating), it automatically locks that line up, turns on the infinity transmitter and all the room conversations coming from that area are heard over this telephone. Of course, we could have tape recording capability on the monitoring side.

You will notice the phone will ring; John will pick it up.

MR. HERSHMAN: This is the type device that rings the phone as opposed to the one where you will cut off the ring before it even sounds?

MR. FAHY: Yes, sir, there are two configurations. This (indicating) cuts off the ring. Immediately after returning the receiver to the cradle I will activate the harmonica bug by blowing the one tone into the transmitter (demonstrating).

The infinity transmitter just turned on. I will try to demonstrate how effective it is by holding it next to the microphone.

MR. HERSHMAN: So, in other words, any conversation in that part of the room will be picked up by the telephone?

MR. FAHY: It is coming over this, yes, sir.

MR. HERSHMAN: And this is a device specifically used for the interception of oral communications within a room, is that correct?

MR. FAHY: That is correct. It has currently been advertised as a burglar alarm system.

MR. HERSHMAN: This is the device that is currently on the market as a burglar alarm system?

MR. FAHY: Yes.

MR. HERSHMAN: Would you explain how it is advertised?

MR. FAHY: It is being advertised to the public as a means of being sure your home is secure when you are away by implanting the infinity transmitter and from a remote location activating it to determine if there are any noises in your premises.

MR. HERSHMAN: They advertise you are able to catch a burglar in the process?

MR. FAHY: Yes.

MR. HERSHMAN: And you are supposed to call at just the right time when he is in the room where the device is and hear his activities?

MR. FAHY: Yes, hoping he will be making some noise.

MR. HERSHMAN: Are there better burglar alarms on the market than that, sir?

MR. FAHY: Yes.

MR. HERSHMAN: So would you say this offer of the infinity transmitter as a burglar alarm is a guise for—

MR. FAHY: Yes, I consider it a farce.

MR. HERSHMAN: Mr. Fahy, if an individual decides to make an outgoing call—

MR. FAHY: One problem is that this device holds the line open. Should somebody try to call the line, they would receive a busy signal. Should the subject attempt to make an outgoing call, you could deactivate the monitoring device by returning the receiver to the cradle on the monitoring side.

MR. HERSHMAN: Mr. Fahy, you have had 20 years' experience and I notice they were spent with the Organized Crime Section of the New York Po-

lice Department. Have you ever had occasion to use an infinity transmitter?

MR. FAHY: No, sir.

MR. HERSHMAN: May I ask why?

MR. FAHY: The limitations, as we discussed before. It does lock the telephone line up.

For any extensive monitoring, the instrument where it is installed can't receive incoming calls or make outgoing calls.

MR. HERSHMAN: Would you consider it a useful device for monitoring one-party consent conversations?

MR. FAHY: No, sir.

MR. HERSHMAN: So here again we are talking about a device used for interception of oral communications?

MR. FAHY: Yes.

MR. HERSHMAN: How sophisticated would you consider this device?

MR. FAHY: It is not sophisticated in that there are various ways of discovering it, but it is sophisticated in the job it will do.

MR. HERSHMAN: How much do they cost?

MR. FAHY: Up to \$600.

MR. HERSHMAN: Can you call any place in the United States to the subject phone and monitor his conversations?

MR. FAHY: Yes.

MR. HERSHMAN: So if you lived in New York and I wanted to monitor your room conversations from California, I could do so?

MR. FAHY: Yes, sir.

MR. HERSHMAN: What is the length of time for installation?

MR. FAHY: It does require entry into the premises. It does not necessarily have to be installed in or near the phone. It can be attached anywhere across the telephone lines within the premises. There is no battery requirement so it doesn't require reentry to change the battery.

MR. HERSHMAN: It is powered off the telephone current?

MR. FAHY: Yes.

MR. HERSHMAN: All right, could we go on to the next device, please.

MR. FAHY: This is out Tri-tap transmitter. As you note, it looks similar to something you buy in a hardware store to plug into your AC outlet to give you three additional outlets. However, this has been modified by being taken apart and an RF transmitter being placed in it with two small holes used for audio pick up (indicating).

When this is placed into an AC line it effectively will transmit through the air a radio signal to any receiver in the area which is set on the same frequency.

MR. HERSHMAN: I assume this is installed in a room to monitor the room conversations?

MR. FAHY: That is correct. We are now getting our room conversations over the receiver.

MR. FAHY: Yes. It looks like an ordinary socket that can be purchased in a hardware store or electrical store.

MR. HERSHMAN: What does something like that cost, Mr. Fahy?

MR. FAHY: These cost \$500.

MR. HERSHMAN: And how far can that broadcast?

MR. FAHY: Again, this has no radiating antenna so the range is limited. I would say a block to a block and a half.

MR. HERSHMAN: What would be the installation time?

MR. FAHY: As fast as it takes to get the device plugged into an A.C. outlet.

MR. HERSHMAN: You would have to be certain that that matched the interior of the room; is that correct?

MR. FAHY: Yes, to some degree. It is a real fast installation.

MR. HERSHMAN: But visual inspection by an ordinary individual would not reveal that that is anything other than a wall socket?

MR. FAHY: No, sir. It even has the manufacturer's name on it. It is available in any hardware store.

MR. HERSHMAN: How would a knowledgeable individual determine that that was not the real thing?

MR. FAHY: If he had a radio receiver that was set on the same frequency as the device he would get a whistle or feedback.

MR. HERSHMAN: There is no need to return to change batteries?

MR. FAHY: No. Once it is plugged in, that is all.

MR. HERSHMAN: And all you need at the other end is an FM receiver?

MR. FAHY: That is correct.

MR. HERSHMAN: And can an FM receiver simply be a modified radio purchased on the market today?

MR. FAHY: Yes.

MR. HERSHMAN: Mr. Fahy, would it be economical to use that for monitoring one-party-consent situations?

MR. FAHY: I have heard of this device being used for a protection situation, possibly for agent protection in a narcotics buy—placed in a motel room for officers to monitor nearby to be sure he is not getting into trouble.

MR. HERSHMAN: Would it be well advised to use that other than other one-party consent devices?

MR. FAHY: At close range I would say yes.

MR. HERSHMAN: Thank you.

Could we go on to the next device, please.

MR. VANDEWERKER: Mr. Hershman, next we have a series of radio transmitters I would like to describe.

The largest transmitter is an example of what we call a drop-in or quick-plant device. What this means is that it is relatively small and can be easily carried into an area to be surveilled. It operates normally under battery power. And once implanted, a device such as this one (indicating) would operate for two to three days, up to a week, depending on power output.

MR. HERSHMAN: Would you hold it up so the Commission can see it?

MR. VANDEWERKER: Yes.

MR. HERSHMAN: Thank you.

MR. VANDEWERKER: This particular transmitter is unlike the others in one respect, in that it has a voice-actuated relay contained internally. This allows for battery conservation since it does not radiate or transmit unless there is audio present in the premises. In that case a transmitter might last for several weeks if it is planted in an office where there is little conversation.

MR. HERSHMAN: I see that is powered by a battery; is that correct?

MR. VANDEWERKER: Yes, it is.

MR. HERSHMAN: How long will that battery last?

MR. VANDEWERKER: This is again a function of how much on time this transmitter has. If it were on continuously it might transmit for one to two days. However, in an intermittent operation, such as in this room today, it would not transmit during the pauses of speech, and thereby conserve its energy. In this situation it might last several weeks.

MR. HERSHMAN: This is a room bug that can be hidden under furniture, behind furniture, or implanted in a wall; is that correct?

MR. VANDEWERKER: Exactly. It can be placed in the backs or cushions of furniture, inside walls upon removal of a power plate or switch outlet, or placed behind a picture frame. There are a number of ways this transmitter could be concealed, including artifacts, various lamps, electrical appliances and fixtures, whatever would be convenient and fit the office decor.

MR. HERSHMAN: What type of broadcasting range does it have?

MR. VANDEWERKER: According to the manufacturer, this transmitter will transmit up to one-half mile. It has a good antenna on it and if installed properly, not close to large metal objects, and the antenna is allowed to extend its full length, and if

the transmitter is operating in a relatively quiet environment, it might be effective for this distance. However, in New York City where the ambient RF energy is high, the effective range might be only a fraction of one city block.

MR. HERSHMAN: And aside from visual detection, how easily detectable is it by countermeasure means?

MR. VANDEWERKER: This particular transmitter, because of its circuitry, might not be detected if there is no sound in the room at the time a countermeasures team were running through their sweep. However, because of its power output, if the transmitter is on at the particular time the countermeasures team were conducting their search, it would be readily detectable.

MR. HERSHMAN: And how much does a device like that cost?

MR. VANDEWERKER: Devices such as this might cost up to \$700.

MR. HERSHMAN: Thank you.

Can we go on to the next device.

MR. VANDEWERKER: Certainly. The next transmitter is manufactured locally and is a good example of a basement manufacturer. This particular transmitter is a microwave transmitter (indicating). It operates at 1,500 megaHertz, which is in the microwave region. It is above many field strength meters, and countermeasure receivers. It does have certain limitations in that it will not transmit through walls, building materials, concrete, etc. Therefore, it is usable principally in a line-of-sight application. A transmitter such as this could be used if it were implanted close to the exterior surface of a building, and shielding somewhat on the interior side to prevent detection.

In this case, this small transmitter would be good for perhaps a quarter of a mile in a short range, line-of-sight situation.

MR. HERSHMAN: What is the advantage of having a microwave transmitter over those you have just shown us?

MR. VANDEWERKER: It is less detectable by conventional countermeasures. The receiving equipment necessary is more sophisticated than that commonly used. The sniffer or fieldstrength measuring device frequently would pass up a device operating in this frequency range due to its lack of sensitivity operating in this higher frequency region.

MR. HERSHMAN: Is the quality of communications received better than those received in lower frequency bands?

MR. VANDEWERKER: The quality of the communications can actually be better because of the lack of radio interference at these frequencies. The lower frequency transmitters frequently have to

compete with commercial broadcast transmitters, emergency services and police communications. However, by moving up into the microwave spectrum, the only thing to compete with is things such as aircraft radar and these types of transmissions.

Therefore, in a short-range path, this transmitter could be put into a quiet portion of the spectrum and thereby transmit very good quality audio.

And this is naturally one of the reasons that the telephone company, itself, uses microwaves across country of large amounts of information.

MR. HERSHMAN: How is that device powered?

MR. VANDEWERKER: This particular device is battery powered.

MR. HERSHMAN: And so its length of operation would depend upon the battery, itself?

MR. VANDEWERKER: That is correct. In many installations, if the size were not prohibitive, many batteries could be used to allow it to operate continuously for a lengthy period of time, perhaps up to a month. However, if you add to this device a voice-controlled or voice-actuated power supply, the length of operation could be extended up to several months.

MR. HERSHMAN: Do you consider that a sophisticated device?

MR. VANDEWERKER: I consider this a fairly sophisticated device from the standpoint of its small size and frequency of operation.

MR. HERSHMAN: Would you expect that to be a device which is used in the private sector by, say, private investigators or other individuals engaged in illegal wiretapping or electronic surveillance?

MR. VANDEWERKER: This device was fabricated by an individual in his basement with a limited amount of materials and for that very reason I would say that there is a chance that devices of this nature could be fabricated by skilled engineers with the appropriate amount of laboratory equipment.

Now, in the industrial sector I would not expect to see devices of this nature operating, not only because of the fabrication techniques but because of the high-frequency receiving equipment required which frequently places it beyond the convenience of FM radios and readily available communications receivers.

MR. HERSHMAN: Can you possibly give us an idea of what something like that would cost with a receiver?

MR. VANDEWERKER: This particular device, itself, would cost approximately \$2,000. The receiver required to intercept this device, if it were limited in range, might cost a similar amount, to perhaps \$4,000, making a total package of \$5,000 to \$7,000.

MR. HERSHMAN: And how long would it take to install something of that nature?

MR. VANDEWERKER: This device would require skillful installation for it to operate properly. It would require alignment, careful placement of the antenna, and some shielding internal to the room. The line of sight would have to be ascertained between the target area and the listening post and any materials in the way of the transmission would have to be removed or the device would have to be replaced in another area.

MR. HERSHMAN: Fine; thank you.

Could we go on to the next device.

MR. VANDEWERKER: This next one is a general-purpose device, approximately the size of a postage stamp (indicating).

MR. HERSHMAN: Mr. Vandewerker, would you please exhibit that for the Commission? You say it is about the size of a postage stamp?

MR. VANDEWERKER: That is correct. It was manufactured by the same individual who manufactured the previous one. The frequency is controllable in this device to operate between 85 and 150 megaHertz, to allow the eavesdropper to adjust his frequency to that portion of the spectrum where he can have a clear channel for communications.

This transmitter can be used as a beacon device and not as an audio intercept device. Because of its small size and with the addition of small batteries this transmitter could be placed in small objects thought to be attractive to a thief, and thereby, if stolen, this transmitter could be remotely located over some limited range.

Transmitters of this size frequently put out only one to two milliwatts which might make them usable in a relatively clean environment for only two to five blocks.

MR. HERSHMAN: For picking up audio?

MR. VANDEWERKER: For picking up audio or tracking if it were being used as a beacon transmitter.

MR. HERSHMAN: I assume that is battery powered?

MR. VANDEWERKER: Yes, it is.

MR. HERSHMAN: Can the output be increased by increasing your power source?

MR. VANDEWERKER: The output can sometimes be increased by increasing the voltage of the power source. Its operating life can be greatly increased by doubling the battery supply available to it and if size is no restriction, this certainly would be done.

MR. HERSHMAN: As compared with other commercially available eavesdropping devices would you consider that a sophisticated device?

MR. VANDEWERKER: I would say that in the industrial sector this would be a sophisticated transmitter and also for law enforcement. It is perhaps one-quarter the size of those devices I have identified produced by other manufacturers during the study.

MR. HERSHMAN: Fine.

Could we go to the next one.

MR. VANDEWERKER: This next transmitter we are calling the Aspirin Tablet transmitter.

MR. HERSHMAN: That is an incredible size. Could you hold up the aspirin tablet next to that?

MR. VANDEWERKER: This (indicating) is the aspirin tablet.

MR. HERSHMAN: Does that transmitter include a microphone and a battery with it?

MR. VANDEWERKER: This size includes both the microphone and battery.

MR. HERSHMAN: In other words, the battery is attached to that device right now?

MR. VANDEWERKER: Right now the space is provided for the inclusion of a battery.

MR. HERSHMAN: Do you have a battery?

MR. VANDEWERKER: I have a battery that is not at the moment installed. It is nearly too small to hold up.

MR. HERSHMAN: Is that battery normally used for hearing aid purposes?

MR. VANDEWERKER: This is the battery used in very small electronic circuits, electric watches, and hearing aids.

MR. HERSHMAN: What is the range of that bug?

MR. VANDEWERKER: This transmitter puts out about three-tenths of a milliwatt, which means it would operate in a quiet radio environment to perhaps two blocks. In a noisy environment it might only operate between adjacent rooms.

MR. HERSHMAN: And does that device have adjustable frequency ranges?

MR. VANDEWERKER: Yes. The manufacturer has designed in a very small tunable system into this transmitter, and by using a broom straw he may slide the tuning system back and forth, and thereby change the frequency.

This, too, will operate over 85 to 150 megaHertz.

MR. HERSHMAN: What does something like that cost, Mr. Vandewerker?

MR. VANDEWERKER: This particular device is offered for sale at \$2,000.

MR. HERSHMAN: And would you consider it sophisticated as compared to the other available devices today?

MR. VANDEWERKER: I would consider it sophisticated on two points, its fabrication technique which is thick film hybrid circuitry which is

required to attain the small size; and for its unique tuning capability.

MR. HERSHMAN: This device, then, is really a product of modern technology, is it not?

MR. VANDEWERKER: Yes.

MR. HERSHMAN: Could we have made a device like this ten years ago?

MR. VANDEWERKER: No, sir.

MR. HERSHMAN: And so, since the 1968 law, and the advent of integrated circuitry, these devices are now practical to build; is that correct?

MR. VANDEWERKER: That is correct. The components are readily available to fabricate hybrid systems such as this. The only requirement is the extensive laboratory equipment required for assembly. Actually a device such as this has to be assembled under a microscope.

MR. HERSHMAN: How about installation of a device like that within a room?

MR. VANDEWERKER: Practically anywhere. This transmitter has a short operating life. It could operate a greater length of time if it had a slightly larger battery. It might operate in this condition for only five to eight hours.

MR. HERSHMAN: That looks like a device that could readily be swallowed.

MR. VANDEWERKER: It was originally planned by the manufacturer that this device could be swallowed if it were encapsulated in some non-degradable material. The manufacturer never found a candidate to test it out.

However, he did discuss it with several physicians and they said it was certainly feasible.

The original concept of swallowing this device and radiating from the body is perhaps limited, since a small transmitter transmitting in this frequency range from inside the body would have an extremely limited range, perhaps only of a few feet.

Therefore, the more realistic concept is the swallowing of the transmitter and later use.

MR. HERSHMAN: Thank you. Will you go on.

MS. SHIENTAG: May I see the \$2,000 aspirin and the battery?

Could this be used for health purposes if swallowed, for detection of a malignancy or something of the sort?

MR. VANDEWERKER: It might conceivably be used for something of the sort.

MR. HERSHMAN: These devices will all be available during the noon break for the news media and Commissioners to take a look at.

MS. SHIENTAG: I hope they will be guarded at those prices.

MR. HERSHMAN: May we go on to the next one.

MR. VANDEWERKER: The next device is the Carrier Current transmitter. This is a device that does not propagate its energy through the air. It is not a radiating transmitter. The difference between the carrier current transmitter and the higher-frequency radio devices is that the frequency is so low that it is below the AM broadcast band, so far below that when installed it does not radiate into free space.

What happens is that this particular device will transmit over the power line to which it is plugged in, or any other pair of wires, such as telephone lines or alarm lines. Any other conductor pair could handle it provided it had the proper source.

This transmitter is built into the base of an inexpensive decorator lamp—

MR. HERSHMAN: That is supposed to represent an ordinary lamp in a room; is that correct?

MR. VANDEWERKER: That is right. This lamp or any other electrical appliance is a very good concealment candidate for a transmitter of this nature, because it offers unlimited life and if properly installed is undetectable by the field strength devices and countermeasure receivers which are trying to determine the presence of eavesdropping devices.

MR. HERSHMAN: Does the lamp have to be on for that device to work?

MR. VANDEWERKER: Not necessarily. It depends. It is the option of the installer. In some cases, if the device is installed in a general room-lighting fixture, the fact the lamp was out would indicate no one was present in the room and in that case the transmitter need not be on. However, if the subject came into the room and turned on the light, it would indicate the presence of individuals in the target area and therefore the transmitter would be on.

MR. HERSHMAN: At what point could the transmissions be received?

MR. VANDEWERKER: The transmissions of a carrier current device are generally limited to the length of wire between the transmitter and the first power transformer.

This means that in a residential situation a single residence or series of residences may operate from a single transformer. If this is the case, the carrier current signal would propagate from residence to residence and be easily retrievable in this manner.

However, in an office building, the power transformer frequently is designed so that it provides energy to one-half of the building structure or to specific floors of that structure.

If this is the case, the carrier current energy might be limited only to those office areas.

However, power companies do by-pass the power transformers. This means that a small electrical

component is installed by the power company at the transformer to allow carrier current signals of this sort to circumvent this transformer and propagate to perhaps the next.

When this particular transmitter was demonstrated by the manufacturer it penetrated or circumvented three power transformers because each of these was by-passed by the power company.

MR. HERSHMAN: How long would it take to install a device of that nature?

MR. VANDEWERKER: Only as long as it took to identify the fixture and perhaps modify the fixture or replace it with a duplicate.

MR. HERSHMAN: Would it be economical both costwise and timewise to use a device of that nature for one-party consent monitoring?

MR. VANDEWERKER: This transmitter might be a very attractive alternate to one-party consent monitoring. It is non-alerting. It is quickly implanted and not readily detectable by the normal procedures of a sweep team.

MR. HERSHMAN: And can you think of any legitimate use a device of that nature would have in industry?

MR. VANDEWERKER: I don't visualize any practical use for a device of this nature in the industrial sector except in some wireless intercom devices.

MR. HERSHMAN: Fine. Can we go on, please.

MR. VANDEWERKER: If we may, we would like to demonstrate this carrier current device.

MR. HERSHMAN: We would like very much to see that.

MR. FAHY: We have installed back here (indicating) extension cords to run our monitoring post down to this point. The lamp is now on and we are on the same power line that would be represented by this line here (indicating chart) so should the transmitter be located in the building, we should receive all the room conversations being carried on in here.

As you will notice here, both the AC power and the radio signals travel along the same line. It is brought to the receiving end and demodulated, which means the voice portion is recovered from the signal, where it is amplified and put out through a speaker.

MR. HERSHMAN: What distance from the device would you have to be for it to pick up conversations in a room?

MR. FAHY: This transmitter uses the conventional microphone found in all of these devices, as well as tape recorders currently available on the market. It might readily detect casual conversations up to 25 feet from the microphone.

MR. HERSHMAN: Thank you.

MR. FAHY: This morning before the hearing started we took the liberty of installing a wire along the table here, as you can see (indicating). At the termination point there is a miniature microphone with electronic circuitry secured to the back of it with epoxy.

MR. HERSHMAN: That is a microphone in your hand?

MR. FAHY: Not only the microphone but the circuitry that goes with it.

We have to picture this line as being from the target premises to a listening post which is advertised as being upwards to 25 miles, which gives the capability of picking up room conversations from this area and transmitting it along wires to an area 25 miles away.

We have a radio receiver here to show you how effective this is.

MR. HERSHMAN: Where can that microphone be installed?

MR. FAHY: Anywhere in the target premise that has wires that we can get to our remote listening point.

We are going to prepare a short tape. I am approximately 15 feet away from the microphone, speaking in a normal voice. If we have all our buttons and knobs right, we should be able to hear it back.

MR. HERSHMAN: Can this be activated and deactivated at the listening post?

MR. FAHY: Yes, it can. The power supply is remotely hooked up. It does require some power. In some instances reentry would be needed to replace the power supply but not in this instance. We can supply the power remotely. We can just change our battery and bring the amplification up to its original condition when low battery level is indicated.

[Whereupon, the device was demonstrated.]

MR. HERSHMAN: And you say that can be done 25 miles away?

MR. FAHY: Yes, sir.

MR. HERSHMAN: For the benefit of the audience, Mr. Fahy, could you tell us how big that microphone is, approximately?

MR. FAHY: Yes. That (indicating) is the whole piece right there.

MR. HERSHMAN: It looks to be smaller than a dime.

MR. FAHY: Yes, sir, it would be. It is just a slight bit larger than the aspirin transmitter shown before. It does require hard wire.

MR. HERSHMAN: How long does it take to install it?

MR. FAHY: Depending on the type of sophistication required it might take a matter of 15 minutes to an hour or so. But it does require the presence of

two wires running between the microphone, itself, and a remote location.

MR. HERSHMAN: And how are those wires concealed?

MR. FAHY: They are concealed possibly as telephone wires, spare wires in the premises brought out and connected to spare telephone wires.

MR. HERSHMAN: Thank you.

I wonder if, with the Chairman's permission, we could now go to the light beam transmitter.

How many more devices do we have?

MR. FAHY: Three.

CHAIRMAN ERICKSON: Off the record.

[Discussion off the record.]

MR. FAHY: Our next device is a remote tone activation kit.

MR. HERSHMAN: You say remote tone activation kit?

MR. FAHY: Yes, sir. What this provides is the use of what is called an encoder plugged into a transmitter. When the encoder is triggered it emits a coded signal through the air to a remote receiver. When the remote receiver is activated, a pair of relays are closed and we can perform any amount of functions with it. We can turn on a remote transmitter; we can start a camera in action, or possibly a tape recorder.

Upon the next pulsing of the encoder the equipment can be turned off. So, therefore, we have remote activation of any kind of a device.

This (indicating) is the actual encoder and transmitter, with a push button (indicating).

This (indicating) is the receiving device. The portion that receives the encoded signal operates a relay in here and could effectively turn this transmitter on from up to, I would say, a distance of about two miles away.

Now, should a reason be necessary to turn the transmitter off, one more pulse on the encoder would turn the battery supply off for the transmitter.

MR. HERSHMAN: How difficult would that make it to find the device if it were turned off?

MR. FAHY: If it were turned off, it would be emitting no radio frequency energy and would be quite hard to determine. Of course, a metal detection device could possibly be used if the device were placed in an area where there was no metal present.

MR. HERSHMAN: Thank you.

MR. VANDEWERKER: Briefly I would like to cover two tracking devices.

The first is a transmitter fabricated locally. This transmitter puts out a tone burst at predetermined intervals. It is designed for concealment with any

package so it might be tracked or monitored by an aircraft or a following vehicle.

It is small enough to conceal in many packages.

This transmitter operates at a relatively low frequency, and puts out one watt, peak power, that might be receivable over distances of 20 to 50 miles under proper conditions.

MR. HERSHMAN: Would that be used, say, to track cargoes?

MR. VANDEWERKER: Yes, it would. This particular transmitter was designed for tracking containers.

The next device is a vehicle-trailing system. This tracking transmitter is somewhat larger. It contains batteries, has high peak power output, and two magnets, one on either end to allow the quick implant under the carriage of a car frame.

MR. HERSHMAN: And that would be used for surveillance purposes, in order to tail a car?

MR. VANDEWERKER: It might be used for surveillance purposes. The tracking technology is quickly developing and finding new applications, not only in surveillance but in security work, and mass transit, following of vehicles.

MR. HERSHMAN: In that condition, run by battery power, how long could it last on the underside of an automobile?

MR. VANDEWERKER: Because of its low-duty cycle, that is, a burst of energy is emitted only every three to ten seconds, a device like this might last for two to three days in continuous operation under a car.

The tracking vehicle frequently contains a display, such as this (indicating) which gives the tracker a left-right indication of his position relative to the tracked vehicle or beacon.

It can be used in aircraft or other surface vehicles.

MR. HERSHMAN: Are devices of this nature typically referred to as bumper beepers?

MR. VANDEWERKER: This category of device is referred to as the bumper beeper. It has been around for many years.

MR. HERSHMAN: What would a system like that cost?

MR. VANDEWERKER: This system might cost, including the direction indicator, over \$1,000. It depends on the amount of sophistication in the display at the receiver end which provides the tracker with left-right and range indications to the target vehicle.

MR. HERSHMAN: Thank you.

MR. VANDEWERKER: The last device we would like to show today is the light beam transmitter. This transmitter is assembled, for ease of display, on a single board (indicating).

In this particular case the audio information coming from either telephone lines or from the room is impressed on a light beam. It is extremely directional, which requires that it be installed in line of sight, between the transmitter and the receiver.

This (indicating) is the transmitter in this display. It uses miniature solid state laser diodes for the actual communications link.

MR. HERSHMAN: How does that differ, Mr. VanDewerker, from the well-known laser beam transmitter?

MR. VANDEWERKER: Are you referring to the window pick-off?

MR. HERSHMAN: Yes, the window pick-off laser transmitter.

MR. VANDEWERKER: The window pick-off laser transmitter has been demonstrated in laboratory situations. In this case the laser beam, itself, is used to retrieve minute vibrations which exist in a window or in another article contained in a room where a conversation is taking place.

In this case the laser beam would reflect from the window or from the object internal to the room, back out to the listening post, and thereby carry the audio in that target area to the listening post.

This type of technology requires very sophisticated demodulation and detection equipment.

However, laser beams, themselves, are readily available in laboratory and industrial equipment at quite nominal cost. The high cost of the pickoff system is in the demodulation and signal analysis equipment required at the listening post.

MR. HERSHMAN: Can this light beam transmitter that you are displaying transmit light signals through solid objects?

MR. VANDEWERKER: No, it can't, sir.

MR. HERSHMAN: So it would have to be in line of sight through a window or something of the sort?

MR. VANDEWERKER: This device is characterized much in the fashion of a flashlight. It would have to be aligned very carefully so its beam of invisible light would be received. It does not require sophisticated demodulation equipment. In this example, the receiver is basically a photo-detector at the receiving end.

MR. HERSHMAN: Is that the true size of the receiver?

MR. VANDEWERKER: Yes, it is.

MR. HERSHMAN: And it demodulates the light beam and turns it back into audio energy; is that correct?

MR. VANDEWERKER: That is correct. The received light signal is demodulated and amplified by an audio amplifier, then fed into a tape recorder or earphones for direct monitoring.

This kind of transmitter would find application in installation in the exterior wall of a building under surveillance. The microphone may not be located adjacent to the transmitter, and may be at the end of length of a wire. The transmitter would be virtually undetectable by conventional countermeasures means since detection is only possible using photodetectors and it would require passing the sensor through the beam of energy to determine its presence.

MR. HERSHMAN: Would you say this particular device is sophisticated compared to other devices on the commercial market?

MR. VANDEWERKER: This device is quite sophisticated relative to the other commercial devices. It primarily is attractive for short-range covert communications or overt communications.

In many cases an industry or an organization may wish to communicate information over short ranges between adjacent buildings on other than telephone lines. This particular transmitter would be capable of transmitting television pictures as well as audio or both at the same time over this link. In that case it would not be classified as a clandestine device.

MR. HERSHMAN: How difficult would it be to detect when being used to intercept oral communications?

MR. VANDEWERKER: To detect the presence of the beam would require the physical interjection of a photo-detector into the beam of energy that is being emitted from the transmitter. So that would require essentially scanning the complete outside wall of a suspect area with a properly aligned photo-detector, such that it might intercept the beam of energy and give an alerting signal.

MR. HERSHMAN: Thank you, Mr. Vandewerker.

I want to thank both you and Mr. Fahy for the fine demonstration you have presented this morning.

The equipment will remain out until after the lunch recess.

CHAIRMAN ERICKSON: Are there questions from the Commission?

CHIEF ANDERSEN: No.

CHAIRMAN ERICKSON: Judge Shientag?

MS. SHIENTAG: No, thank you.

CHAIRMAN ERICKSON: Professor Blakey?

PROFESSOR BLAKEY: I would like to ask a question about the laser transmitter you discussed. How large is the equipment that will be required to take sound off a pane of glass?

MR. VANDEWERKER: The laser, itself, might be perhaps the size of this box (indicating).

PROFESSOR BLAKEY: That box is about the size of a shoe box?

MR. VANDEWERKER: Yes, sir, it is.

The receiving and processing equipment might be contained in three boxes of this size at the listening post.

The qualification is necessary because the only place I have seen a laser window pick-off operate is in a laboratory situation.

PROFESSOR BLAKEY: It is not a practical law enforcement tool now?

MR. VANDEWERKER: Not now. It is too costly and susceptible to various problems, such as thermal updrafts, building vibrations, and so on.

PROFESSOR BLAKEY: Thank you.

CHAIRMAN ERICKSON: With your technological background—and you are an expert in this field—could you commercially buy the parts necessary to construct any of these devices?

MR. VANDEWERKER: Yes, sir. Any of these components would be available through the parts houses, catalog houses. You could buy the parts by mail order. The schematic diagrams of many of these types of devices are available in the literature, in library books, documents that have been prepared in the past, and by identifying the components a technician could order the components and with some experimentation actually fabricate many of these devices.

Those requiring a higher level of sophistication such as the laser beam transmitter or microcircuitry devices would be more difficult to produce.

In this case various fabrication equipment is required, which would be out of place for the conventional technician. This equipment might cost upwards of \$10,000.

CHAIRMAN ERICKSON: Are some of the completed devices available on the open market today?

MR. VANDEWERKER: The vehicle tracking transmitters are openly available. They are not considered part of the restricted audio surveillance devices.

The microphone systems are all readily available.

The pre-amplifiers, the control boxes, if required, are certainly available.

The telephone modification systems are radio-TV store type technology. They could be easily duplicated by a relatively unsophisticated technician.

CHAIRMAN ERICKSON: So what we have before us is the fact that many of these devices can be put into electronic or wiretapping use by the relatively unsophisticated technician?

MR. VANDEWERKER: That is correct, sir. The one large source of devices, for example the radio transmitters, might be the off-the-shelf walkie-talkies that are available wherein the individual might simply purchase a walkie-talkie or a pair of walkie-

talkies and disassemble them and reassemble the interior circuitry into another package and simply use that as the drop-in transmitter with its battery power supply and its own microphone, even.

CHAIRMAN ERICKSON: Thank you very much. The Commission is deeply indebted to both of you. The work you have done on the state of the art is going to make our Commission report meaningful and will demonstrate how modern technology has made wiretapping and electronic surveillance possible in today's world.

Thank you very much.

We will take a 45-minute break for lunch and reconvene here at quarter to two. And these devices will remain during the noon hour but we would hope the table would be clear at quarter of two.

We stand recessed.

[Whereupon, at 1:00 p.m., a luncheon recess was taken until 1:45 p.m.]

AFTERNOON SESSION

CHAIRMAN ERICKSON: Ladies and gentlemen, we will commence at this time.

Chief Lynn, will you come forward and be sworn.

[Whereupon, Carrol M. Lynn was sworn by Chairman Erickson.]

TESTIMONY OF CARROL M. LYNN, CHIEF OF POLICE, HOUSTON, TEXAS

CHAIRMAN ERICKSON: The record should reflect that we are about to take the testimony of Carrol M. Lynn, Chief of the Houston Police Department, who will also testify regarding illegal police wiretapping.

Chief Lynn took office in January of 1974, and very soon began to suspect that his home and office telephone lines were tapped. He asked the local FBI office to investigate the taps, but when no action was taken, Chief Lynn began his own inquiry. Today he will outline for us the results of his investigation.

So will you proceed.

MR. LYNN: Yes, sir.

CHAIRMAN ERICKSON: You have an opening statement and that will be filed for the purpose of the record and will be reflected in that manner.

To save time—and I know you recognize that we are taking you out of order in order to facilitate your return in an emergency to Houston—if you would care to summarize that opening statement, we'd be willing to accept the summary—or would you prefer just to read the statement?

MR. LYNN: Either. I can summarize it, if you like.

CHAIRMAN ERICKSON: I think it might be well to summarize the statement.

MR. LYNN: Just in summary, I did take office on January 9, 1974, when we had a new mayor who went into office.

The first signs of any problems in Houston were when two officers in 1973 had been indicted for various charges with strong allegations that wiretapping was involved.

I did become suspicious of my telephones. One reason was that certain information was leaked over the telephones. I did go to the Office of the FBI and ask for assistance. Everything was done that was possible to talk me out of even making a complaint. Finally, when they did take my complaint, it was approximately ten days before two gentlemen came to my office, along with a telephone company man—two men from the FBI—and obviously were not prepared to make an investigation as they indicated it would be very difficult to even inspect my telephone, asking me if I had a screwdriver that they might open it up with.

I recognized at that time that it was rather a joke.

The next thing that did catch my attention was the fact that we did have nine officers who were indicted out of an IRS investigation—not an FBI investigation but an Internal Revenue Service investigation. They were indicted for several charges, one of them being wiretapping.

At that time I did start an investigation.

I was warned prior to the investigation not to do anything, and to be careful what I did, if anything, and what I said, by one of the former members of the Intelligence Division, the former head of the Intelligence Division. He said there were some real big people in Houston—I forget his exact words—that would come down on me hard if I went too hard on this. And I might say he was right.

I did, I believe, talk altogether with six key people that had been in key positions and recorded their conversations.

I would say in summation that the information I learned, including the initial building, deployment, and destruction of the equipment, a follow-up investigation should have been elementary. However, to this date no other indictments have come down and nothing has been done, as far as I know.

CHAIRMAN ERICKSON: The complete statement which you have made is a part of the record. If anyone at the meeting desires to review the entire statement which you have made, it is available.

[The prepared statement of Carrol M. Lynn follows.]

STATEMENT OF CARROL LYNN, CHIEF OF POLICE, HOUSTON, TEXAS

My name is Carrol M. Lynn. I have been the Chief of Police of Houston since January 9, 1974. I have served as a member of the Houston Police Department for 19 years. During the four years immediately prior to becoming chief, I served as Director of the Houston Police Training Academy. The Houston Police Department is one of the largest in the country with over 2,500 officers.

During the summer of 1973, two Houston narcotics division officers were indicted and convicted in State Court for violations of narcotics laws. The allegations arising out of the investigation of these two officers included charges of illegal wiretapping. These officers' convictions were the first public sign that all was not well in the Houston Police Department.

In late 1973, Houston elected a new mayor, Fred Hofheinz, who selected me to serve as his Chief of Police.

Soon after taking office, I became concerned that my own home and office telephones might be tapped. My suspicions were aroused when certain information discussed over my private telephone line was disclosed publicly. A check by a private consultant confirmed that my telephones may have been tapped. Following the consultant's inspection, I notified the F.B.I. special agent in charge in Houston and requested that he initiate an investigation of what I considered a very serious violation of my privacy and of federal law. (Describe this meeting)

In addition to suspicions concerning my own telephone, another incident occurred which increased my concern about illegal wiretapping. Nine Houston police officers were indicted on federal charges which included I.R.S. and wiretapping violations. To date these men have not yet been tried although the indictments were handed down nearly one and a half years ago. These indictments arose out of an Internal Revenue Service investigation centered on an alleged Houston narcotics dealer, not as a result of an F.B.I. investigation, even though the F.B.I. is the agency charged with the enforcement of federal antiwiretap laws.

Finally, I determined to initiate a more thorough investigation of the matter myself. When it became known that such an investigation might be initiated, a former intelligence division supervisor who had left the department paid a call on me and suggested that I watch what I did and said about the officers who had been indicted because I could get into trouble with a number of powerful people in Houston. He also stated that if certain officers started talking they could bury a number of people. A few days later I again met with this individual in my office. However, this time I had arranged to secretly tape record the meeting and to find out more about what the individual knew about illegal wiretapping.

He admitted that he was aware of past wiretapping by the department. When I asked him if the wiretapping was controlled, he stated that his part of it "damned sure" was, but that he didn't think wiretapping by the narcotics division was. He stated that he had discussed his concerns about the narcotics division with former chief of police. In boasting about his own intelligence division's use of wiretapping, he stated, "these people were good at it, and we never had no problems whatsoever. But then, as time went on, hen our people had the technical know-how."

When I asked how they got information about what line to tap, he stated that no one in the division other than he was able to obtain the information so far as he knew, and he obtained it from the phone company. He did not name his source within the phone company, however. When I asked if others, outside the division, had known of the illegal wiretapping he stated:

"Well, there's two F.B.I.'s right over there now that was with us on one deal out here." When I asked if those F.B.I. agents weren't upset by the illegal wiretapping he said: "Didn't do a damned thing about it. Sat there and listened just like everybody else . . ."

Following my recorded conversation with the former intelligence division supervisor, I called in three members of the department's communications division to learn what they knew of the illegal tapping. Two were interviewed separately, then all three together. The interviews with these three individuals revealed that use of wiretapping by the Houston Police department had been going on since 1967 or 1968 and that it had been used by at least four divisions: Narcotics, Intelligence, Vice and Homicide. One of the men estimated that at least 40 to 50 officers were involved.

The wiretapping equipment was manufactured by the communications division. Its use was controlled by means of a log book which individuals checking out equipment had to sign. However, by the time of my interviews the log book and the equipment had been destroyed. When I asked if other agencies were involved in the use of the equipment, I was told that on one occasion the Federal Bureau of Narcotics and Dangerous Drugs had asked for some assistance.

The communications officer stated:

"The Federal Bureau of Narcotics and Dangerous Drugs actually called us from San Antonio and they wanted us to do a schemats (schematic diagram) of our equipment. Our telephones was working far superior to anything they ever had, and I called the former chief myself and said, "Do we cooperate?" He said, "Hell, no."

In addition, I was told equipment was supplied to police in other cities just outside of Houston.

At one point in an interview with one of the communications division officers, I was told that three or four wiretap devices had been picked up by Bell Telephone employees in the course of maintenance. These devices were returned by Bell to the Police Department. Another high ranking officer told me that an illegal police device had been returned to him personally by a top security officer of Southwestern Bell on one occasion.

In addition to the interview I personally conducted and recorded, interviews with the two convicted officers were conducted by a private consultant at my request. The transcripts of these interviews reveal the following. Illegal wiretap evidence was often used in the department for the necessary probable cause to obtain a search warrant, especially in narcotics cases. The warrant application would simply disguise the use of wiretapping by stating that the information came from an unidentified informant. In fact, on some occasions department funds which were reserved for paying informants were actually withdrawn from the departments' account to make it look like an informant had been paid for the information.

These officers stated that Federal Bureau of Narcotics agents and Texas Department of Public Safety officers were, on occasion, involved with Houston Police Department wiretapping. They described one particular narcotics case in which federal agents were involved and stated that one agent warned, "We should not be spreading it out too much that they were involved." The officers stated that federal narcotics agents "were fully aware of wiretaps being conducted by the City."

Further, I was told by one Houston police officer that advance information about a possible federal crackdown on wiretapping was readily passed on to the Houston police. According to this officer the former chief of the narcotics division announced one day at a division staff meeting that a team of F.B.I. investigators would be coming to town to try to "bust" wiretapping. He said that he had had the information passed to him from the chief's office and that wiretapping would be stopped for a while.

Finally, in addition to the interviews I have already described, I conducted one other secretly recorded conversation with the

chief of security for Southwestern Bell in Houston. Although he personally denied giving illegal wiretap information to law enforcement officers since 1966 he admitted to me that he was aware that it was being done and that it was his policy merely to "look the other way."

Mr. Chairman and members of this Commission, in concluding my testimony I would like to observe that in spite of all I have told you there have not been any indictments for illegal wiretapping in Houston other than those returned at the beginning of my term of office which spurred my initial investigation. My investigation, which I turned over to the U.S. Attorney, included the initial building, deployment and destruction of the equipment. A follow-up investigation should have been elementary. It is particularly disturbing to me that, to date, only a few patrolmen, at the bottom of the bureaucratic ladder, have had to face prosecution, while those above them who were equally as involved in illegal wiretapping, including possibly federal agents and telephone company personnel continue to go free.

This concludes my statement.

CHAIRMAN ERICKSON: At this point, I turn the questioning over to the staff, Mike Hershman.

MR. HERSHMAN: Chief Lynn, when exactly did you begin your probe of illegal police wiretapping?

MR. LYNN: I would say it was in the early part of the summer of 1974.

MR. HERSHMAN: In what manner did you conduct this probe?

MR. LYNN: First, with the information I had gathered just from talking with several people, watching the nine people being indicted, and things like this, I talked with my private attorney and pointed out the need to preserve the evidence. And at that time I decided that I would keep a tape of our conversations.

MR. HERSHMAN: So you invited members of your command to speak with you and taped their conversations with you; is that correct?

MR. LYNN: Selected members, yes, sir, six people.

MR. HERSHMAN: Can you tell us briefly what those conversations revealed, sir?

MR. LYNN: It revealed that around 1968 they went—I haven't read the transcripts in several months and they have been turned over to the U.S. attorney in Houston for about nine months now. They went to Colorado, I believe—I am not positive but I believe it was Colorado—bought some of the latest equipment, brought it back and analyzed it and decided they could make it cheaper—as a matter of fact, for almost nothing.

They developed this equipment in the sixth floor of the Police Department, in the Communications Center. They had a log book where officers would sign this wiretapping equipment out.

At first, it apparently was pretty well controlled, with supervisors keeping an eye on it. But it appeared that toward the last, just about anyone

could make the decision on whether to wiretap and who they wanted to wiretap.

After the new mayor took office, the equipment was either burned or it was broken, and some of it was buried, thrown in the bayou.

MR. HERSHMAN: What about the logs concerning the equipment? Are they still intact?

MR. LYNN: The logs? No, they have been destroyed.

MR. HERSHMAN: Do we know who destroyed the logs and equipment?

MR. LYNN: Yes, sir.

MR. HERSHMAN: Were they members of your command?

MR. LYNN: They were.

MR. HERSHMAN: Have they been disciplined in any manner?

MR. LYNN: The only discipline that I could take—well, actually I could personally take no discipline because of the state law that says that anything that happens must have happened within the past six months. This is providing that the person is not either indicted or found guilty of an offense. Then you can take action regardless of how long it is. But I have found myself in the position of not being able to take action against the majority of the people.

MR. HERSHMAN: Can you tell us, Chief Lynn, approximately how many members of the Houston Police Department were involved in illegal wiretapping?

MR. LYNN: From talking to the people who should know, probably between 40 and 50.

MR. HERSHMAN: Were they all capable of installing and operating this equipment?

MR. LYNN: Yes.

MR. HERSHMAN: For what purposes did they put this equipment to use?

MR. LYNN: Apparently in the beginning it was put to police work in the area of narcotics and vice and gathering intelligence. But it seemed that as time went on it became more lax and individual patrolmen would make their own minds up as to what they wanted to do with it.

MR. HERSHMAN: And was it an effective tool when they used it, even illegally?

MR. LYNN: Well, that is a debatable question.

In 1974, with all the problems that we had, with the indictments that went down—I didn't even know why at the time; the reason I started my investigation.

We reorganized our Vice Division and our Narcotics Division. Our Vice Division in Houston made more felony or vice arrests than all of the major cities in Texas combined—and those are the big ones, the ones that count. Our Narcotics Division made

so many arrests that we had to add new chemists. Where before they were sending about 400 cases a month, they started sending in 700 cases a month in 1974, doing everything legally—an awful lot of hard work but everything was legal.

MR. HERSHMAN: Can you tell us of any specific cases where illegal eavesdropping was used?

MR. LYNN: Probably on some pieces of some. There are some that are under trial at this time that I know something about, and it might jeopardize the cases.

CHAIRMAN ERICKSON: Regarding the cases on trial, I would prefer that you did not relate it.

MR. LYNN: Thank you, sir.

A number of the ones I know about will, I fear, be on trial at some time.

CHAIRMAN ERICKSON: Is it possible for you to testify about them in such a way that you could refer to them by incident and not identify them by name?

MR. LYNN: All right, sir.

I talked with one officer and he told me of a case where they had a wiretap on a gentleman's phone for over a month continually. And during this period of time, many officers came and went from this location.

The man was a trafficker in narcotics. He sold a lot of narcotics in Houston. However, they did not arrest him. And I asked him why, and he said, "Well, we could get all of the little people that was coming and going and it was very easy to catch them, and it made our arrest records look better."

I found that peculiar, personally, but I believe he was telling the truth.

MR. HERSHMAN: Was the use of illegal wiretapping confined to the Narcotics Division?

MR. LYNN: No, sir. From what I have been told, it was used by Narcotics, by Vice, by what is known as Criminal Intelligence, and by Homicide.

MR. HERSHMAN: Were the products of these illegal wiretaps used to commit other crimes?

MR. LYNN: Again, I have been told—I can give you one story that would relate it probably better. This officer told me that he was attempting to get out of the Narcotics Division. He realized that he was in over his head and that some day there might be a reckoning. And he said—well, I asked him to give me a specific on why he wanted out so bad. He said, "One day my commander called me in and he had several names. And he said, "I want these people put in jail or the penitentiary." He wanted them put away.

He said, "Boy, if you don't know how to put them away, I'll put you back on three wheels," which is a demotion in status, not a demotion in pay.

I asked him what he did. He said, "The first thing I did was put a tap on their phones." And he said, "Some of them were dealing a little bit in narcotics."

I said, "What about the others?"

He grinned and said, "We always carry narcotics in our pocket. If you can't get them one way, you get them another."

If I might make this observation, I believe when anyone in a position of supervision asks a police officer to commit a crime as serious as this violation is, then they cannot expect them to stop at that one crime. Because this is a crime that they might justify as saying, "We are trying to better society," but it does carry a penalty of five years and a \$10,000 fine. So why shouldn't he commit a crime that would benefit himself personally?

And this is the danger, as I see it, in what really happened in Houston.

MR. HERSHMAN: Were your officers aware that when they engaged in an illegal wiretapping they were committing a crime?

MR. LYNN: I would have to say yes, that they were.

MR. HERSHMAN: Did you get the indication that perhaps they believed the risk was not as great as the possible rewards?

MR. LYNN: I never heard them talking about the rewards so much at that time. It had been done for such a long period of time and so many people were doing it that it was just taken as a way of life. No one really, I think, at a certain point even worried about it.

MR. HERSHMAN: Now, Chief Lynn, there is no state authorization statute in Texas, is there—

MR. LYNN: No, sir, there is not.

MR. HERSHMAN: —that would permit court-authorized wiretapping?

MR. LYNN: No, sir.

MR. HERSHMAN: So in effect any wiretapping or bugging done by police officers in Texas would be illegal; is that right?

MR. LYNN: Yes, sir, that is correct.

MR. HERSHMAN: When was this information concerning illegal wiretapping by police officers in the Houston Police Department turned over to the U.S. attorney's office?

MR. LYNN: It was the latter part of 1974 that I met with them and turned it over.

MR. HERSHMAN: And have there been any indictments to this time concerning illegal wiretapping?

MR. LYNN: No, sir, there have not.

MR. HERSHMAN: Who has conducted the investigation of illegal wiretapping for the U.S. attorney's office?

MR. LYNN: It is my understanding that the Federal Bureau of Investigation has conducted this.

MR. HERSHMAN: Has the fact that the Federal Bureau of Investigation maintained close liaison with the Houston Police Department affected in any way that investigation?

MR. LYNN: In my opinion, yes.

MR. HERSHMAN: Why is that?

MR. LYNN: Well, I think it's kind of the code of the West. You don't ever rat on a brother officer. And I think that they feel close in this and it makes it very difficult for them to make—and I can understand their position. It makes it very difficult for them to make the investigation.

MR. HERSHMAN: In your conversations during your internal investigation, were there indications that federal officers knew of or participated in illegal wiretapping?

MR. LYNN: Yes, sir, there was.

MR. HERSHMAN: Would you explain what circumstances existed?

MR. LYNN: I was told that in one case two FBI agents walked in while they were tapping a phone and were getting information at that time.

In another case, I was told that, I believe it was the Bureau of Narcotics—I believe is what it was—had called and had asked if they could see a schematic diagram of our equipment. It seems that we did a very good job in Houston and we built some real good equipment. And they were refused the diagrams and the equipment.

MR. HERSHMAN: I believe in your statement you mentioned that officers within the Houston Police Department were given advance warning on the wiretap investigation by the Federal Bureau of Investigation.

MR. LYNN: Yes, sir. I was told that at one point the commander of the Narcotics Division came down and simply said something to the effect that it had come from the Chief's office that all wiretapping would stop; that they had information that a team of federal men or FBI men—I forget which—would be coming into the city to look at it. And everything stopped for awhile.

MR. HERSHMAN: Do you believe, Chief Lynn, that this wiretapping was going on prior to 1968?

MR. LYNN: Yes, sir, I do.

MR. HERSHMAN: Do you believe there were any precautions taken once the Federal Wiretapping Act was passed in 1968?

MR. LYNN: Well, it appears that somewhere around the time that a lot of sophisticated equipment came out, it just accelerated, from what information I have been able to get.

MR. HERSHMAN: Do you have any indications from the individuals you spoke with of telephone company involvement or participation?

MR. LYNN: That they did get—I believe they call it the pair numbers, where to tie it in at, from people in the telephone company. Sometimes they got it from the Security Department; sometimes they got it from linemen. It seemed to be a commonplace thing to find someone in a position who committed a crime in the telephone company and to hold this over their head while they furnished them information. So it seemed in these two ways they were able to get all the information.

MR. HERSHMAN: Did you have a conversation with the Chief of Security of Southwest Bell in Houston?

MR. LYNN: Yes, sir, I did.

MR. HERSHMAN: Did you tape that conversation?

MR. LYNN: I did.

MR. HERSHMAN: What did the conversation reflect?

MR. LYNN: It seemed that up to 1966 he did give out information. But he said in 1966 orders came down for it to be stopped. He stated that he was well aware that it was going on, that members in the Department had even gone so far as to ask him if he had minded, and he told them, "So long as I don't know about it," and in effect what he did was just turn his head. This is what he said.

MR. HERSHMAN: What would happen, Chief Lynn, if telephone company employees discovered wiretap devices placed on a line by Houston police officers?

MR. LYNN: In several cases I learned that they simply brought them back to the police department.

MR. HERSHMAN: And they would not report that find to the Federal Bureau of Investigation?

MR. LYNN: Apparently not, due to the fact they just brought it back and gave it to someone in the department.

MR. HERSHMAN: Was there a particular liaison in the department who contacted the telephone company for needed information?

MR. LYNN: I think that probably there were a couple of people. They didn't bring it back just to anyone. There were probably a couple of divisions that it was brought to more often.

MR. HERSHMAN: Can we estimate how many wiretaps or buggings were done since 1968 by Houston police officers?

MR. LYNN: I was asked that same question by Senator Tower in Texas, and I really don't know, except to say that it apparently was a very common everyday occurrence, and that it would be numerous.

MR. HERSHMAN: The individuals who ran the Narcotics Division, the Vice Division, the com-

manding officers—were they aware of the wiretap activity?

MR. LYNN: Yes.

MR. HERSHMAN: Were some of the fruits of the wiretap activity used for the obtaining of search warrants and such?

MR. LYNN: I was told that to get the probable cause they would use this, and of course, make up a story. And in the big cases that were made, they would learn where it was, and then they would, of course, go forth with a different type of information and get their search warrant to make the raid or whatever it was.

MR. HERSHMAN: Is there any indication that local prosecutors were aware of the source of that information?

MR. LYNN: I was told by communications officers that they were.

MR. HERSHMAN: I have no further questions.

Thank you.

CHAIRMAN ERICKSON: Chief Andersen.

MR. ANDERSEN: Is wiretapping illegal in Texas aside from the Federal Code? Is it an illegal act in Texas to wiretap.

MR. LYNN: Well, the fact that we don't have any type of law—it would be illegal, yes, sir.

MR. ANDERSEN: But you have no specific statute?

MR. LYNN: It is my understanding we have nothing at all.

MR. ANDERSEN: Were you on the Houston Police Department before you were appointed Chief?

MR. LYNN: I have been there 19 years; yes, sir.

MR. ANDERSEN: Were you in any of these sections during that 19 years?

MR. LYNN: No, sir, I was not.

MR. ANDERSEN: Was this common knowledge through the Department during these years?

MR. LYNN: Towards the last. The last couple of years you heard a lot of rumors. Many of them, in the position I was in as Director of the Training Academy, I didn't quite believe, and I took them just as rumors.

MR. ANDERSEN: Can I presume you have an internal affairs or internal security unit?

MR. LYNN: We do not.

MR. ANDERSEN: You do not have an internal investigations unit?

MR. LYNN: We do not.

MR. ANDERSEN: I was curious why your own unit didn't investigate it. But you do not have such a unit within the Houston P.D.?

MR. LYNN: No, sir, we do not.

MR. ANDERSEN: Is there any question on this? Did any of these officers do this for personal gain? Is there any evidence of personal gain?

MR. LYNN: I believe in some of the indictments that have already been handed down, evidence of personal gain has been set forth as part of the gain.

MR. ANDERSEN: Personal profit or graft or whatever terminology you want to use?

MR. LYNN: Yes, such things as taking money off the narcotics dealers, and things like this.

MR. ANDERSEN: When you originally suspected your own phones, did you ask Southern Bell to routinely sweep all your phones?

MR. LYNN: No, sir, I went to the office of the FBI.

MR. ANDERSEN: You went to the FBI, not to the telephone company first?

MR. LYNN: That is correct.

MR. ANDERSEN: I have no more questions.

CHAIRMAN ERICKSON: Judge Shientag.

MS. SHIENTAG: Just one or two questions, Mr. Chairman.

Did you ever learn why your wires were tapped?

MR. LYNN: Not absolutely for sure, no, I did not.

MS. SHIENTAG: What did you suspect was the reason?

MR. LYNN: Well, I would suspect they wanted to know what a new chief was going to do.

MS. SHIENTAG: When you say "they," you mean the FBI?

MR. LYNN: I would assume that a number of people would probably want to know what we might be thinking about doing in some cases.

MS. SHIENTAG: When you say "number of people," enforcement agencies, federal or state?

MR. LYNN: Well, I would only be guessing if I said that.

MS. SHIENTAG: Well, you are making a statement.

MR. LYNN: I never did find out for sure who it was.

MS. SHIENTAG: Who he was?

MR. LYNN: Who was checking them.

MS. SHIENTAG: You are the Chief of Police there?

MR. LYNN: Yes, ma'am.

MS. SHIENTAG: Do you suspect it was non-law enforcement individuals who might have been making the taps on your wire?

MR. LYNN: It could have been either.

MS. SHIENTAG: You think it could have been some organized crime source?

MR. LYNN: That had crossed my mind as well.

MS. SHIENTAG: Well, beyond crossing your mind, did you take any action as Chief of Police to ascertain the truth of this?

MR. LYNN: Well, I went as far as I believe could be gone as far as asking that the lines be checked.

Shortly after they were checked, it appeared that the taps were taken off. And I don't know how you would discover who was doing it.

MS. SHIENTAG: Is there a local district attorney there?

MR. LYNN: Yes, Ma'am.

MS. SHIENTAG: Did you speak to him about prosecuting the alleged wiretappers?

MR. LYNN: We had a long discussion about this, we sure did.

MS. SHIENTAG: And what happened?

MR. LYNN: He made the statement that on his telephone, any time that he used it, he made sure that he never said anything on it that he wouldn't just as soon be in the newspaper.

MS. SHIENTAG: That is all, Mr. Chairman.

CHAIRMAN ERICKSON: Professor Blakey.

MR. BLAKEY: Chief, you testified that you did not have an internal affairs section in the Department in 1966, and I take it your testimony is you do not have one now.

MR. LYNN: That is correct.

MR. BLAKEY: And yet, you have reorganized the Department following these scandals.

MR. LYNN: Right.

MR. BLAKEY: Who investigates corrupt policemen in Houston?

MR. LYNN: We still use a system where the person who they work for, the person they are responsible to, makes the investigation.

MR. BLAKEY: Do you think that is a good way to do it?

MR. LYNN: In theory, it places the responsibility where it should be, in a semi-military organization.

MR. BLAKEY: Supposing the responsibility has not been fulfilled, as apparently it has not been in the past in Houston.

MR. LYNN: I would say regardless of the system that you set up, if the people at the top didn't want it to work it wouldn't work.

MR. BLAKEY: That is true, but would you grant me that some systems work a little better than others?

MR. LYNN: I think so, yes, sir.

MR. BLAKEY: And your testimony is that you have approximately 2,500 sworn officers in Houston.

MR. LYNN: That is true.

MR. BLAKEY: That makes you one of the larger police departments in the country.

MR. LYNN: Yes, sir.

MR. BLAKEY: Do you think there are many others similarly organized without inspection divisions?

MR. LYNN: That large? I don't know of any that doesn't have an internal affairs unit.

MR. BLAKEY: Hasn't this problem, or perhaps our conversation, now led you to reconsider the organization of your department?

MR. LYNN: I have considered it for a long time, that one phase. And I think that at some time it will have to be done. There are so many people that are against the idea that timing on it would be a very important thing.

MR. BLAKEY: Maybe the thing to do would be to just let them resign. It seems to me what you are describing is the leadership positions in most of your major divisions were aware of this and allowing it to go on. It was widespread.

You have had a major problem of corruption in Houston.

MR. LYNN: We are talking about before 1974.

MR. BLAKEY: You have the same people now. You have told us you cannot discipline them because of the six-months' statute of limitation. Do we have any guarantee your people are not doing it now?

MR. LYNN: I do not have the same people in any of the sensitive divisions.

MR. BLAKEY: The same people are on the street, aren't they?

MR. LYNN: Many of them have taken sick time—they got sick and decided to wait it out to see if I don't stumble and fall, and then they will come back if I do.

We have a very strong state law where discipline of a Houston police officer is very difficult.

MR. BLAKEY: I suspect it would be difficult if you have no investigative body in Houston to uncover evidence.

MR. LYNN: Of course, we have the grand juries.

MR. BLAKEY: Do they have independent investigators assigned to them?

MR. LYNN: They can have, but not necessarily.

MR. BLAKEY: Routinely they do not?

MR. LYNN: Routinely, no.

MR. BLAKEY: Does the D.A.'s office in Houston have an investigative squad?

MR. LYNN: I believe that they do have some investigators or they use—they do have some investigative ability.

MR. BLAKEY: Am I correct in assuming that they primarily perfect cases that you already bring to them?

MR. LYNN: I'm sorry.

MR. BLAKEY: Am I correct in assuming they primarily perfect cases that you bring to them? They don't do independent investigations on their own, do they?

MR. LYNN: In some cases, they do.

MR. BLAKEY: But rarely?

MR. LYNN: I don't know how often it is but in some cases they do.

MR. BLAKEY: How many investigators do they have?

MR. LYNN: I really don't know.

MR. BLAKEY: Less than 100?

MR. LYNN: Oh, yes.

MR. BLAKEY: Less than 50?

MR. LYNN: I would say so.

MR. BLAKEY: Less than 25?

MR. LYNN: Probably.

MR. BLAKEY: Is there any other law enforcement agency with state authority acting in Houston?

MR. LYNN: Well, in Houston, Texas, of course, you do have the Sheriff's Department.

MR. BLAKEY: Does he have criminal jurisdiction, or is he a process server?

MR. LYNN: Both. He does some police work and he does—I would assume—

MR. BLAKEY: Did you ever have a corruption case made against the Houston Police Department by the Sheriff's Department?

MR. LYNN: No.

MR. BLAKEY: Do you have state police?

MR. LYNN: Yes.

MR. BLAKEY: Do they have arrest power?

MR. LYNN: Yes.

MR. BLAKEY: Do they operate in Houston without your permission?

MR. LYNN: We have a good working relationship with them.

MR. BLAKEY: Can they come in without your permission?

MR. LYNN: In Houston, Texas? Oh, sure.

MR. BLAKEY: Do they routinely do it?

MR. LYNN: They would notify us of anything on a large scale.

MR. BLAKEY: Have they ever conducted a corruption investigation of your department?

MR. LYNN: No.

MR. BLAKEY: Chief, if I understand your testimony, you are really down there on your own. Nobody watches the Houston Police Department, do they?

MR. LYNN: Well, I would say that the people at the top do.

MR. BLAKEY: They haven't in the past.

MR. LYNN: No, they haven't, as close as they should.

MR. BLAKEY: What guarantee will the people of Houston and the rest of the country have that they will not do it again in the future?

MR. LYNN: I think the only guarantee they can have is by who the mayor is, how he feels about it, who the chief is and how he feels about it.

MR. BLAKEY: But there is no institutional mechanism in Houston to watch the watchers; correct?

MR. LYNN: Other than what we have discussed, no, sir.

MR. BLAKEY: Chief, you commented, frankly, adversely on the relationship between your Department and the FBI in the sense that they didn't conduct an investigation of your people because they didn't want to—I think your phrase was—rat on a fellow officer.

Is that a quote from an FBI agent?

MR. LYNN: No, that is my quote.

MR. BLAKEY: Have you ever talked to an FBI agent about your department and discussed specifically the quality of their investigation of your department?

MR. LYNN: I have talked with a few FBI agents about it, yes.

MR. BLAKEY: In what capacity? Have you talked to the SAC?

MR. LYNN: The ones that are apparently working on this particular case.

MR. BLAKEY: Would you know the case agents that are assigned to this case?

MR. LYNN: I know them when I see them. As a matter of fact, I talked with them very briefly Friday.

MR. BLAKEY: Has he ever expressed to you the feeling that he wouldn't conduct an investigation of your department if he had indications of violation of the law?

MR. LYNN: No.

MR. BLAKEY: Has any other FBI agent expressed that feeling to you?

MR. LYNN: No.

MR. BLAKEY: Why do you put words in their mouths, then, to say they wouldn't investigate a fellow officer?

MR. LYNN: I only go by what has happened over a length of time.

MR. BLAKEY: This is your inference based on circumstantial evidence?

MR. LYNN: And I believe I pointed that out, yes, sir.

MR. BLAKEY: You don't have direct statements by any officer in an official capacity that says he is not or will not conduct an investigation of your department?

MR. LYNN: I would say that he would be a very, very stupid officer to make a statement like that.

MR. BLAKEY: Or he might be honest, or not intend it, et cetera.

MR. LYNN: It is possible.

MR. BLAKEY: Have Bureau agents conducted interviews of your department people?

MR. LYNN: Some.

MR. BLAKEY: And have your department people been called before federal grand juries?

MR. LYNN: Some have.

MR. BLAKEY: Have you had occasion to discuss this investigation with the United States attorney?

MR. LYNN: Yes, I have.

MR. BLAKEY: Has he ever expressed an opinion to you that he would not prosecute?

MR. LYNN: No, he has not.

MR. BLAKEY: You recognize, of course, that your statement leaves this Commission with the impression that the Department of Justice is not taking action in Houston.

MR. LYNN: I can only go by the fact, sir, that they have not taken action.

MR. BLAKEY: Well, they have not taken an action yet. Do you have any indication that they are not moving this case through their processes, however laborious?

MR. LYNN: I would say that the follow-up investigation that they had should have been completed within—

MR. BLAKEY: Is that a Monday morning quarterback judgment?

MR. LYNN: That is my judgment, sir.

MR. BLAKEY: But you haven't gotten from them a declination of prosecution?

MR. LYNN: I'm sorry.

MR. BLAKEY: You have not gotten from them an indication that they are not going to prosecute?

MR. LYNN: No, I would not make such a statement, of course not.

MR. BLAKEY: You leave us with the impression they are not going to do it. Is it your impression they are not doing it fast enough to suit you or not doing it at all?

MR. LYNN: I think after the length of time the information has been there, I would wonder why some action has not been taken.

MR. BLAKEY: Aren't you free to take the same information to your own grand juries?

MR. LYNN: Oh, no.

MR. BLAKEY: Why not?

MR. LYNN: It is strictly a federal case.

MR. BLAKEY: There is no conceivable violation of the Texas Code—invasion of privacy, trespass, malicious mischief—that this could not be brought before a state grand jury?

MR. LYNN: There is not at this point that I know of.

MR. BLAKEY: Have you discussed this with your local prosecutor?

MR. LYNN: I have discussed it with the D.A.

MR. BLAKEY: And has he given you an indication that he would not prosecute the people?

MR. LYNN: He prosecuted two people.

MR. BLAKEY: For what?

MR. LYNN: I believe the broad terms, as I recall, were—it was in '73 before I took the job. I believe they were theft, as I recall.

MR. BLAKEY: You have indicated that some of the officers used this wiretap information to extort narcotics dealers; correct?

MR. LYNN: This is what I have been told, sir.

MR. BLAKEY: Let's pin down what you mean when you say you have been told. By whom have you been told?

MR. LYNN: The person or persons that told me that are, as a matter of fact, probably fixing to go to trial right now on another case.

MR. BLAKEY: Is extortion a crime in Texas under the Texas Code?

MR. LYNN: It probably would be, yes, sir.

MR. BLAKEY: Or at least grand larceny, if they have actually received the money?

MR. LYNN: They have already been prosecuted for some type of a theft charge.

MR. BLAKEY: So there has been action by some people in prosecuting some of these police officers?

MR. LYNN: There has been some action, yes, sir.

MR. BLAKEY: Has your department played a role of any kind in investigating the grand theft or extortion?

MR. LYNN: That was before I became chief and apparently they did some, yes.

MR. BLAKEY: Has it been done since you were Chief?

MR. LYNN: We have made a number of investigations.

MR. BLAKEY: Have they produced any indictments?

MR. LYNN: At this time, no.

MR. BLAKEY: How long have you been conducting your investigations?

MR. LYNN: I started this part of the investigation that we are talking about on the wiretapping—

MR. BLAKEY: You have got a problem that runs a little deeper than wiretapping. You have police officers extorting people. I'd say it's a little deeper than wiretapping; it's extortion.

MR. LYNN: When I first took over as Chief of Police, sir, I made a number of investigations. I had a number of people resign immediately.

MR. BLAKEY: How long have you been Chief?

MR. LYNN: A year-and-a-half.

MR. BLAKEY: And you have been conducting investigations for a year-and-a-half.

As a result of your investigations, have there been any state indictments returned? Have your people made any arrests of your own people?

MR. LYNN: Yes, sir. I can't recall all of them, but we received state indictments on some, yes.

MR. BLAKEY: Then the impression you are leaving us that nothing is being done is not really very accurate, is it?

MR. LYNN: It is very accurate, sir. We are talking about two different things.

MR. BLAKEY: I take it we are talking about corruption in the Houston Police Department. Are we talking about anything else?

MR. LYNN: As far as corruption in the Houston Police Department, we are actively and have actively investigated it, and I do not believe at this time that we have a great deal. I think Houston today has probably one of the cleanest departments in the nation.

MR. BLAKEY: The same people?

MR. LYNN: Many of them are still there. They are not in sensitive divisions.

MR. BLAKEY: What indication do you have that these people have reformed?

MR. LYNN: Well, I doubt very seriously that they have reformed.

MR. BLAKEY: Do you have the identity of the two FBI agents who allegedly walked in on an illegal tap?

MR. LYNN: I don't have them—

MR. BLAKEY: I am not asking you for them but simply do you have them?

MR. LYNN: I don't have them with me today.

MR. BLAKEY: Have you ever had their names and addresses?

MR. LYNN: I know who one of them was, yes, sir.

MR. BLAKEY: And what was the character of the information that you had to indicate he walked into it? An eye witness?

MR. LYNN: Yes, sir.

MR. BLAKEY: Did you make a specific complaint to the Bureau indicating that specific Special Agent Blank walked in on an illegal wiretap?

MR. LYNN: No, sir, I turned it over to the U.S. attorney's office.

MR. BLAKEY: Is that special agent still in the Houston area?

MR. LYNN: Yes, sir, he is.

MR. BLAKEY: Is there any indication he has been disciplined?

MR. LYNN: No, sir, there is not.

MR. BLAKEY: Do you know the identities of the BNDD agents that were specifically involved in illegal wiretapping?

MR. LYNN: I do not know them, no, sir.

MR. BLAKEY: Did you have the names or did you just simply have a rumor to that effect?

MR. LYNN: I did not obtain the names at that time.

MR. BLAKEY: Have you obtained them since?

MR. LYNN: No, sir.

MR. BLAKEY: So you don't know the identity of the BNDD agents?

MR. LYNN: You see, I am not an attorney—

MR. BLAKEY: I am just asking you factual questions. I am not asking you anything about the law.

MR. LYNN: —and I took the advice of my attorney about at what point to turn this over to the U.S. attorney's office.

MR. BLAKEY: Chief, I am asking you, did you know the names of the people or did you not know their names?

MR. LYNN: As far as I recall, I don't recall their names.

MR. BLAKEY: Did you make any specific investigation further to determine who they were?

MR. LYNN: No, sir.

MR. BLAKEY: What was the character of the information that came to you indicating they were BNDD agents? Did you have an eye witness?

MR. LYNN: On DEA agents?

MR. BLAKEY: Yes.

MR. LYNN: One was what I talked about earlier, a telephone call.

MR. BLAKEY: Did you get the name and address of the person who said he saw a federal narcotics agent?

MR. LYNN: That information is in the hands of the U.S. attorney at this time, yes.

MR. BLAKEY: Did you get any indication that the DEA has taken any disciplinary action?

MR. LYNN: I have not.

MR. BLAKEY: Mr. Chairman, I'd like to ask that the staff communicate with the Department of Justice and the FBI and the Bureau of Narcotics to find out what action, if any, has been taken in prosecuting these cases and processing them with reference to the discipline of these agents.

I'd also like to ask that the answers to those communications be incorporated in the record at this point.

[The material referred to follows.]

UNITED STATES DEPARTMENT OF JUSTICE

FEDERAL BUREAU OF INVESTIGATION
WASHINGTON, D.C. 20535

July 10, 1975

General Kenneth Hodson
Executive Director

National Commission for the Review of Federal and State Laws
Relating to Wiretapping and Electronic Surveillance
1875 Connecticut Avenue, N. W.
Washington, D. C. 20009

Dear General Hodson:

Information has come to the attention of this Bureau that Mr. Carrol M. Lynn, former Chief of Police, Houston, Texas, who resigned June 26, 1975, and Mr. Anthony J. P. Farris, former United States Attorney, Houston, Texas, appeared before the Commission and testified on June 25, 1975. The testimony included their allegation that an investigation of illegal wiretaps by

the Houston Office of the Federal Bureau of Investigation (FBI) was not actively pursued because it involved the Houston police. Their testimony also included an allegation that two FBI Agents stationed in Houston had walked in on an illegal wiretap being manned by the Houston police and did nothing about it.

These same allegations were previously made by Mr. Farris and Mr. Lynn when they testified before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the Committee on the Judiciary, House of Representatives, on May 22, 1975, and have been repeated numerous times in the news media. In January, 1975, then Deputy Attorney General Laurence H. Silberman advised of similar allegations having been made against Houston FBI Agents in connection with their investigation of alleged illegal electronic surveillance activity by the Houston Police Department (HOPD).

A comprehensive inquiry into these allegations was conducted in accordance with Mr. Silberman's request. The results of this investigation established that these allegations of misconduct were totally unfounded. The inquiry revealed nothing which could be considered substantial delay or lack of willingness on the part of FBI personnel to pursue all logical investigative avenues available. The inquiry revealed no FBI personnel had any association with or personal knowledge of illegal electronic surveillances by the HOPD. The inquiry revealed no indication that the Houston Office of the FBI had ever engaged in any illegal electronic surveillances.

In view of the fact that the allegation concerning illegal wiretapping on the part of the HOPD is the subject of an ongoing investigation by the FBI, I cannot comment further concerning that investigation.

The above is being furnished to you in order that the correct facts concerning these unfounded allegations of misconduct may be placed on record with your Commission.

Sincerely yours,

[Signed] Clarence M. Kelley,
Director

MR. BLAKEY: And I'd also like to express my serious reservation about the presentation of this kind of testimony which casts serious doubt on the integrity of the Department of Justice and people in it unless it can be accompanied at the time the allegation is made with an opportunity for those people or institutions or individuals whose reputations are being blackened to respond at the time and at the place.

If I take the Chief's testimony at face value—and I do—some very serious things have been put in our record, and it seems to me the people against whom they cut ought to have an opportunity to answer.

Frankly, it seems to me it is unfair not to do this.

CHAIRMAN ERICKSON: Professor Blakey, I am advised by staff and I have been informed that the Federal Bureau of Investigation has been contacted; that they have indicated they would not comment on an ongoing investigation. So the inquiries are being made, and hopefully we will obtain the information.

MR. BLAKEY: Mr. Chairman, let me clarify. It is not the comment on the investigation of the wiretapping. I am, of course, interested in hearing that the Department of Justice is processing it.

But I am concerned that we have said the two specific federal agents, identified FBI agents, have been in a situation where they participated in an unlawful wiretap, and at least one of the agents is still in place in Houston. I'd like to find out whether the FBI has made an administrative investigation of that agent for internal discipline. And if they have not, it seems to me they should be called to account for it.

And if they have made it and the evidence indicates that the allegations are false or there is a reasonable explanation for it, it seems to me our record ought to indicate, however that situation turns out, and frankly I think it should have indicated it at the same time this witness' testimony was put in the record.

CHAIRMAN ERICKSON: I might state this witness has previously appeared before Congressman Kastenmeier, who is a member of this Commission. The material presented to Congressman Kastenmeier was largely made available to him by our staff, and our staff has been pursuing this vigorously, and hopefully we will be able to complete our investigation into this.

Chief, if I might ask a few questions, you were with the Houston Police Department 19 years, as I understand it?

MR. LYNN: That is approximately correct, yes.

CHAIRMAN ERICKSON: And in that course of time, you probably had occasion to serve on nearly every division within the Department?

MR. LYNN: Several divisions, yes, sir.

CHAIRMAN ERICKSON: And as I understand it, at least four divisions, you discovered, had been involved in illegal wiretapping activities?

MR. LYNN: Yes, sir.

CHAIRMAN ERICKSON: Have you ever served on any one of those divisions?

MR. LYNN: Yes, sir, I had. Homicide.

CHAIRMAN ERICKSON: And in connection with the homicide investigations, they had been using illegal electronic surveillance equipment?

MR. LYNN: It seems that the best information that I have on that is they would usually get another division to actually do the technical work for them; they were not technically oriented themselves.

CHAIRMAN ERICKSON: So they were calling in another division to do it for the Homicide Division?

MR. LYNN: Yes, sir, that is about my information.

CHAIRMAN ERICKSON: When you were in Homicide, they didn't do it that way?

MR. LYNN: No, sir, they did not. I was a homicide detective for a little over four years, and it was all hard work and lots of leg work.

CHAIRMAN ERICKSON: Now, when you talk about the equipment that you had, I understand that some of that was sold to other law enforcement agencies in Texas.

MR. LYNN: As far as I know, we bought a piece of equipment and had our technicians tear it down. And then they saw what it contained, and I believe the statement was even made, "We could build a better piece than this is." And we built our own and continually built our own equipment for Houston Police Department use.

CHAIRMAN ERICKSON: But this was sold to other law enforcement agencies, was it not? Doesn't your opening statement say that?

MR. LYNN: No, sir. I don't believe that we ever sold—at least I have no information that we ever sold our equipment.

CHAIRMAN ERICKSON: Well, did you supply it to police in other cities outside of Houston?

MR. LYNN: Yes, sir. It appears that some police in other cities did check it out and use it.

CHAIRMAN ERICKSON: Was that after you became Chief?

MR. LYNN: Oh, no, sir.

CHAIRMAN ERICKSON: Now, what is your hierarchy of command in Houston? The Chief is in charge of the Department?

MR. LYNN: Yes, sir.

CHAIRMAN ERICKSON: And you have department heads immediately beneath you?

MR. LYNN: That is correct.

CHAIRMAN ERICKSON: And they report to you?

MR. LYNN: That is correct.

CHAIRMAN ERICKSON: When you found out about this wiretapping going on and the fact that your own phone was tapped, did you talk to them about it?

MR. LYNN: The department heads that we had—none of them were over these three sensitive areas of narcotics and and vice and criminal intelligence. Those three answered directly to the Chief.

CHAIRMAN ERICKSON: So the only person that these three divisions had to answer to was the Chief himself?

MR. LYNN: That is correct. I did change that structure and put a deputy chief over those three divisions.

CHAIRMAN ERICKSON: So the Chief that was in office prior to the time that you were there was the one that was in charge of these three groups that were carrying out this illegal surveillance?

MR. LYNN: Yes, sir, that is correct.

CHAIRMAN ERICKSON: And is he still with the Houston Police Department?

MR. LYNN: No, sir, he is not.

CHAIRMAN ERICKSON: And his name, of course, was turned over to the FBI if he was the one that was in charge of those divisions.

MR. LYNN: His name was turned over, yes, sir.

CHAIRMAN ERICKSON: And the heads of those divisions were identified?

MR. LYNN: Yes, sir.

CHAIRMAN ERICKSON: Are any of those four division heads still with the Houston Police Department?

MR. LYNN: I believe two of them are.

CHAIRMAN ERICKSON: Have you questioned those division heads about their knowledge about the illegal acts that were being conducted by their divisions?

MR. LYNN: Yes, sir.

CHAIRMAN ERICKSON: And I presume you took statements from them?

MR. LYNN: I don't believe that they would give a statement. I did tape record one of them.

CHAIRMAN ERICKSON: Did you give them the *Miranda* warnings in view of the fact that this did involve criminal activity?

MR. LYNN: No, sir, I did not.

CHAIRMAN ERICKSON: Did you think that the finger of guilt, if you will, pointed at them, that they were involved in this?

MR. LYNN: At that point I was simply exploring to see where it did go and how deep it went.

CHAIRMAN ERICKSON: Well, at that point you knew that there had been wiretapping?

MR. LYNN: I knew there had been. Yes, sir, I knew there had been wiretapping.

CHAIRMAN ERICKSON: Did you ever see the log that you referred to in your opening statement?

MR. LYNN: No, sir.

CHAIRMAN ERICKSON: How do you know those logs existed?

MR. LYNN: People that handled the logs, that were in charge of them, have told me.

CHAIRMAN ERICKSON: And those people are still with the police department?

MR. LYNN: They are still with the police department. They have appeared, most of them, I believe, before the federal grand jury.

CHAIRMAN ERICKSON: The logs that they were to keep were part of the Houston police records?

MR. LYNN: Yes, sir, I would say so.

CHAIRMAN ERICKSON: And those have been destroyed?

MR. LYNN: Yes, sir.

CHAIRMAN ERICKSON: You taped the interviews that you had with one or two of these division chiefs by using some type of a monitoring device concealed on your person?

MR. LYNN: That is correct.

CHAIRMAN ERICKSON: A body mike, as they call it?

MR. LYNN: I used a body mike, and I used a plain tape recorder.

CHAIRMAN ERICKSON: And they didn't know you were taking the statement from them?

MR. LYNN: That is correct.

CHAIRMAN ERICKSON: Did they admit that they had conducted these tests?

MR. LYNN: Oh, yes.

CHAIRMAN ERICKSON: And did they say how many times they had used this illegal electronic surveillance?

MR. LYNN: I really don't recall any specific number.

CHAIRMAN ERICKSON: Well, did they indicate the period of time that this practice had been followed?

MR. LYNN: It seems in '67 and '68 it had been going on pretty regularly, I was told.

CHAIRMAN ERICKSON: Did it go on after that?

MR. LYNN: Up until 1973, when it appeared that a new mayor was coming on the scene. The former head—well, he was the head of the Intelligence Division at that time—stated that he personally supervised the burning and the busting and the burying of this equipment.

CHAIRMAN ERICKSON: Professor Blakey asked you about the names of these federal drug agents and the members of the Federal Bureau of Investigation. Did you have the names of the actual agents that were involved?

MR. LYNN: I don't recall if the names were on there or not. As I said, I haven't read those transcripts in nine months, and I don't recall if they were on the transcripts or not.

CHAIRMAN ERICKSON: I am not asking about whether it was on the transcripts. I am just asking if you ever knew the names of the federal agents that participated in this illegal electronic surveillance?

MR. LYNN: I am sure the names were given to me at one time. I believe that they are in the hands of the U.S. attorney's office at this time. But I personally don't recall.

CHAIRMAN ERICKSON: Do you remember the name of the officer that gave you the identity of the four others?

MR. LYNN: I recall the officer, yes, sir.

CHAIRMAN ERICKSON: do you remember the officer of the Houston Police Department who told you?

MR. LYNN: Yes, sir.

CHAIRMAN ERICKSON: And he is still working for you?

MR. LYNN: That particular officer, no, sir.

CHAIRMAN ERICKSON: He is not with the Houston Police Department?

MR. LYNN: No, sir, he is not.

CHAIRMAN ERICKSON: Was he terminated because of this participation in this activity?

MR. LYNN: For a different reason. He was terminated for a different reason. It wasn't for the wiretapping.

CHAIRMAN ERICKSON: But it was for some improper conduct?

MR. LYNN: Yes, sir.

CHAIRMAN ERICKSON: In pursuing the investigation as to these federal agents, did you turn over their names to the special agent in charge of the Federal Bureau of Investigation in Houston?

MR. LYNN: To him—no, sir, I did not.

CHAIRMAN ERICKSON: You didn't turn it over to the special agent in charge?

MR. LYNN: No, sir.

CHAIRMAN ERICKSON: They have an internal investigation unit, do they not, the Federal Bureau of Investigation—or do you know?

MR. LYNN: I am not familiar with that.

CHAIRMAN ERICKSON: Did you talk to the Texas Rangers about this?

MR. LYNN: No.

CHAIRMAN ERICKSON: Did you talk to Carroll Vance, the district attorney?

MR. LYNN: We did discuss it, yes.

CHAIRMAN ERICKSON: I know Mr. Vance has a rather competent investigating unit of his own. Did you ask the assistance of the district attorney's investigation team to go into your Houston Police Department to assist in ferreting out this illicit activity?

MR. LYNN: We talked about—I had a long visit with Carroll on this. And frankly, he had already faced a lot of heat in the fact he had indicted two Houston police officers. And I guess you might say he had come under a lot of fire in Houston for it.

And he stated, at that point, unless concrete evidence was brought to him, he was not going to participate in internal affairs of the Houston Police Department any further.

CHAIRMAN ERICKSON: Well, did you give him concrete evidence?

MR. LYNN: We have on some other cases.

CHAIRMAN ERICKSON: I am not asking about other cases. I am asking about this wiretapping. Did you tell him what you have told this Commission, largely that there was illicit wiretapping going on within the Houston Police Department and it had been going on and that you wanted something done about it?

MR. LYNN: We discussed it but I don't believe I asked him to do anything about it. I don't believe it was in his jurisdiction. This is what I was told.

CHAIRMAN ERICKSON: You went to the U.S. attorney?

MR. LYNN: That is correct.

CHAIRMAN ERICKSON: Did you make this request of him?

MR. LYNN: I did. I turned over to the U.S. attorney my findings.

CHAIRMAN ERICKSON: Your findings?

MR. LYNN: That is correct.

CHAIRMAN ERICKSON: What do you mean by "findings?" Is that your conclusions?

MR. LYNN: That was all of the conversations that I had had with the officers that I had talked with, and we worked for a length of time very closely with him, turning over certain reports that tied in with the different information.

CHAIRMAN ERICKSON: Was this a written summary of what you had learned, or did it contain the statements or the product of your investigation? Or what was it? Just a complaint as to what you believed occurred, or did it go farther than that? Did you offer the case like you would offer it when you turned it over to the district attorney for prosecution, say, on a narcotics case? You'd turn over statements; you'd turn over how the information came into your hands, with dates, times, places, circumstances. Did you detail it in that manner?

MR. LYNN: It was detailed in that manner over a period of several days.

I went over first at the end of 1974 and talked, I believe, with Mr. Farris who is here now. And we discussed the problem as it had existed long before I was there. He was very interested in any information I had, in anything that I had done that would assist them.

CHAIRMAN ERICKSON: He was cooperative?

MR. LYNN: Oh, most definitely. And I explained to him what I had done and why I had done it like that. And we agreed that we would work together. And I did then bring in this information to them, and some of my people then worked with some of his people on updating many things, such as cases—there was a lot of information.

CHAIRMAN ERICKSON: Were any of the witnesses that you gave him called before a grand jury?

MR. LYNN: Yes, sir.

CHAIRMAN ERICKSON: So a grand jury investigation has been underway?

MR. LYNN: Yes, sir.

CHAIRMAN ERICKSON: Chief, I very much appreciate your giving us your time and offering us the information.

The material that you have included in your opening statement is true and constitutes your statement as to the summary of the events.

MR. BLAKEY: Mr. Chairman, I wonder if I could ask one more question.

Chief, during this period of time your people did not have wiretapping authority from the state legislature; is that correct?

MR. LYNN: That is correct, sir.

MR. BLAKEY: If they wanted to do this legally, they could not have done it legally; is that correct?

MR. LYNN: That is my understanding of the law.

MR. BLAKEY: And you say you have been an officer in the Houston Department for about 19 years?

MR. LYNN: Yes.

MR. BLAKEY: Would you say you are generally familiar with the attitudes and values of the men in that department?

MR. LYNN: Generally, yes.

MR. BLAKEY: Do you think that if they had a lawful way of doing it, that is, if the state had passed a statute authorizing it to be done under a court-ordered system, they still would have engaged in this illegal conduct?

MR. LYNN: I think it would probably have made a big difference if they had had the lawful means of doing it.

MR. BLAKEY: So in a sense this all could have been avoided if your state had carefully drafted in the post-1968 era a wiretapping statute like Title III?

MR. LYNN: Yes, sir, I believe so.

MR. BLAKEY: Thank you.

CHAIRMAN ERICKSON: Chief, thank you very much for coming, and I hope the work that you have done will result in the improvement of our wiretapping structure and we can see an end to illegal wiretapping.

Thank you again for coming.

We now call as our next witness Mr. Anthony Farris.

[Whereupon, Anthony J. P. Farris was sworn by Chairman Erickson.]

TESTIMONY OF ANTHONY J. P. FARRIS, FORMER U.S. ATTORNEY, SOUTHERN DISTRICT OF TEXAS

CHAIRMAN ERICKSON: The record should reflect that Mr. Anthony J. P. Farris, former U.S. attorney for the Southern District of Texas, is now prepared to testify.

He held that office from February of 1969 until his resignation in December of 1974. During that time, Mr. Farris became aware of extensive illegal wiretapping being carried out by members of the Houston Police Department, but his efforts to involve the local FBI offices in the full investigation were not as successful as he believed they should have been.

Mr. Farris will discuss his role in the disclosure of the illegal activities in Houston.

Mr. Farris, I will now allow the staff to conduct the preliminary investigation, and we do appreciate your waiting so patiently to give your testimony to this Commission.

MR. FARRIS: Thank you, Mr. Chairman.

MR. HERSHMAN: Mr. Farris, do you have an opening statement?

MR. FARRIS: A very brief one. I know that you have a copy of my opening statement that I made to the House Subcommittee, but I would like to give a summary, if you will, of where this started and what it was like when I left office, December 30, 1974.

The matter actually started in the investigation by the IRS of a large heroin dealer in 1971. We ended up getting a conviction on this dope peddler. That investigation by the IRS then led into the subsequent investigation into illegal wiretapping, civil rights violations, tax evasion, rip-offs of small-time narcotics peddlers, and so forth.

The matter then culminated in a joint indictment of nine past and present Houston Police Department officers.

This was early in 1974 when they were indicted. Because of a technicality, they had to be reindicted again in two separate bills in May of 1974.

Subsequent to that, we discovered that they were represented by the same three lawyers that were representing not only them but several witnesses. This made a horrible conflict of interest apparent. We brought this to the attention of Judge Allen B. Hannay, who then directed that those lawyers must go, and that the nine inditees immediately get new lawyers.

The matter was appealed to the Fifth Circuit Court of Appeals, and it is pending before them, thus preventing the U.S. Attorney's office from prosecuting those officers.

In the process of investigating that matter, the IRS discovered that there appeared to be a lot of rumors and allegations of illegal wiretapping by various members of the HPD.

I wanted the IRS to continue the investigation, but since this was an 18 U.S.C. violation, Commissioner Alexander would not let them do this, so obviously the matter had to be decided by the FBI investigators.

The FBI had various indications of the allegations of illegal wiretapping by the HPD as far back as the late summer or early fall of 1973. To my knowledge, when I wrote to them in April of '74 and asked them formally to follow their charter and investigate the matter, they had not up to that point commenced an investigation. They assigned one agent to investigate the matter, and it dragged on

until I left office in December of 1974, during which time I had sent various letters to the SAC, letters, notes, telephone calls, what have you, with copies to the General Crimes Section in Washington.

In December of 1974, after I had had a visit from Chief Lynn, I sent a lengthy letter to General Saxbe with copies to the Deputy Attorney General and a copy to the then Chief of the Criminal Division, Henry Petersen, pointing out that there was this reluctance by the local FBI to thoroughly and comprehensively investigate this matter; that it was dragging on; that there were 2500 officers over there suffering because some 40 or 50 had allegedly committed this federal offense.

To my knowledge, I learned later that the response was forthcoming from Justice sometime in the latter part of January. Justice has never directly interviewed me to hear from me my reason for alleging that the FBI had, in effect, dragged its feet in this matter. To this point they have not done it, even though I testified to this effect before Chairman Kastenmeier's committee a month ago.

MR. HERSHMAN: Thank you, Mr. Farris.

I wonder if you could tell us how many agents are assigned to the FBI's field office in Houston?

MR. FARRIS: The office there is, of course, headquartered in Houston, but they also have Beaumont, which is some 90 miles from Houston, and Corpus Christi, which is some 200 miles, included in the Houston office. They have slightly in excess of 100 agents.

MR. HERSHMAN: And when you requested they initiate a formal investigation, how many agents did they assign to that investigation?

MR. FARRIS: One.

MR. HERSHMAN: And you had discussions with that agent about the investigation?

MR. FARRIS: No. The Assistant Chief of the Criminal Division in my office, Ronald J. Waska, had various discussions with them—some of them in blunt terms—all to no avail.

MR. HERSHMAN: Did they submit reports to you on their investigative findings?

MR. FARRIS: If you call them reports.

MR. HERSHMAN: What did they consist of? How would you characterize them?

MR. FARRIS: I can't go into them, except that they were brief and had no meat.

MR. HERSHMAN: In some cases did they consist of nothing more than newspaper articles?

MR. FARRIS: Yes.

MR. HERSHMAN: What basically did you say in your letter to Attorney General Saxbe?

MR. FARRIS: I reviewed the whole matter, as I did here—

CHAIRMAN ERICKSON: For the sake of the record, your letter of December 17, 1974, to General Saxbe can be included as part of the record. And I believe it already has been received.
[The letter, dated December 17, 1974, follows.]

UNITED STATES DEPARTMENT OF JUSTICE

UNITED STATES ATTORNEY
Southern District of Texas
12000 Federal Building
and U.S. Court House
515 Rusk Avenue
Houston, Texas 77002
P.O. Box 61129, HOUSTON, TEXAS 77061
December 17, 1974

Honorable William Saxbe
Attorney General
U.S. Department of Justice
Washington, D.C. 20530

Re: Houston, Texas Police Department;

Violation of Title 18 U.S.C. 2510, et seq.

F.B.I. Bureau File Reference 139-4467

F.B.I. Field Office File Reference 139-189

Dear Mr. Saxbe:

In June of 1971, the Criminal Intelligence Division of the Internal Revenue Service, Houston, Texas, commenced an extensive income tax investigation of Sebastian Mirelez, a large heroin dealer in Houston, Texas. This investigation culminated in the conviction of Sebastian Mirelez and the imposition of a sentence of six years imprisonment. Further investigation, with the assistance of Sebastian Mirelez, resulted in the conviction of a former Houston, Texas Police Officer for perjury before a federal grand jury. With the assistance of the convicted officer, indictments were returned charging nine (9) additional Houston, Texas Undercover Narcotics Officers with income tax evasion, civil rights violations and narcotics violations. These cases are presently pending trial. The success of these matters is related directly to the performance of Criminal Intelligence Agents I. A. Filer, Jack Hollingshead, Don Nettles and Frank Zapalac of Houston, Texas. The dedicated, conscientious and competent efforts of these agents are unequalled in my experience as United States Attorney for the Southern District of Texas. Sebastian Mirelez dealt narcotics on a major scale on the streets of Houston, Texas, for years, apparently with purchased immunity from the Houston Police Department, Narcotics Division. All the Narcotics Officers indicted were veteran officers who worked in an undercover capacity. Needless to say, the apprehension of these individuals required labor beyond traditional investigation.

During the course of the income tax investigation, allegations arose reflecting the illegal interception of communications by the Houston, Texas Police Department. A portion of these allegations ripened to fruition and are contained as charges in the civil rights Indictment presently pending trial. The Federal Bureau of Investigation is currently investigating the new allegations of illegal interception of communications.

On November 19, 1974, the new Chief of Police of Houston, Texas, Carrol M. Lynn and the new Captain of the Narcotics Division, B. G. Bond, delivered information to this office which confirmed our greatest fear that the Houston, Texas Police Department had utilized illegal electronic surveillance on a large

scale. While useful and conclusive, the information in no way amounts to evidence sufficient to meet the burden of proof in Federal District Court. It is my opinion that an immediate and exhaustive investigation may result in evidence sufficient to present before a federal grand jury under Title 18, United States Code, Section 2510 et seq.—Interception of Communications. The information further *confirms positively* that the interests of society and justice, which are synonymous in my mind, could not be served by allowing the Federal Bureau of Investigation to investigate this matter.

To provide you with complete background information on the captioned subject enclosed are the following:

(1) Letter from Harris County District Attorney Carol S. Vance to Anthony J. P. Farris, United States Attorney, dated November 20, 1973, advising this office that allegations of illegal interception of communications by the Houston, Texas Police Department have already been presented to Tom Jordan, Special Agent in Charge, Federal Bureau of Investigation, Houston, Texas, by the Harris County District Attorney's Staff. Until the moment of receipt of this letter on November 23, 1973, this office had not been advised either by the Harris County District Attorney or the Federal Bureau of Investigation of the existence of such allegations. This letter is marked as *Exhibit 1*.

(2) Original referral letter dated April 29, 1974, from Ronald J. Waska, Assistant Chief, Criminal Division, Assistant United States Attorney to Mr. Thomas Jordan, Special Agent in Charge, Federal Bureau of Investigation requesting "that a comprehensive investigation commence immediately." Please note that this office furnished as enclosures to the F.B.I. four (4) alleged illegally intercepted tape recordings and a nine (9) page sworn affidavit by a former Houston Police Officer admitting the rampant utilization of interception devices by the Houston Police Department. This letter is marked as *Exhibit 2*.

(3) Letter dated September 12, 1974, from Ronald J. Waska, Assistant United States Attorney, Assistant Chief, Criminal Division to Mr. Robert Russ Franck, Special Agent in Charge, Federal Bureau of Investigation enclosing a newspaper article from the Houston Post dated September 12, 1974, describing an *admission* by a former police officer, Carlos Avila, that illegal interception devices were utilized by the Houston, Texas Police Department. This letter is marked as *Exhibit 3*.

(4) Letter dated September 12, 1974, from Ronald J. Waska, Assistant United States Attorney, Assistant Chief, Criminal Division to Mr. Robert Russ Franck, Special Agent in Charge, Federal Bureau of Investigation enclosing two newspaper articles from the Houston Post and the Houston Chronicle further describing *admissions* by former Houston, Texas Police Officer Carlos Avila and Assistant District Attorney Bob Bennett, that illegal interception devices were utilized by the Houston, Texas Police Department. This letter is marked as *Exhibit 4*.

(5) Letter dated September 23, 1974, from Ronald J. Waska, Assistant United States Attorney, Assistant Chief, Criminal Division to Mr. Robert Russ Franck, Special Agent in Charge, Federal Bureau of Investigation enclosing two newspaper articles from the Houston Post and the Houston Chronicle dated September 21, 1974, describing the setting aside of marihuana convictions because the convictions were supported by evidence obtained as the result of illegal interceptions conducted by the Houston, Texas Police Department. This letter is marked as *Exhibit 5*.

(6) Letter dated September 25, 1974, from Ronald J. Waska, Assistant United States Attorney, Assistant Chief, Criminal Division to Mr. Robert Russ Franck, Special Agent in Charge, Federal Bureau of Investigation enclosing two (2) motions filed by the Harris County District Attorney's Office, Houston, Texas, and two (2) orders executed by a State District Judge setting aside marihuana convictions because the Houston, Texas Police Department gathered evidence through the use of illegal interception devices. This letter is marked as *Exhibit 6*.

(7) Letter dated October 31, 1974, from Ronald J. Waska, Assistant United States Attorney, Assistant Chief, Criminal Division to Mr. Robert Russ Franck, Special Agent in Charge, Federal Bureau of Investigation correcting an erroneous assertion on an F.B.I. Report and again referring to our request for "an exhaustive and diligent investigation of these serious allegations." This letter is marked as *Exhibit 7*.

(8) Excerpts of tape-recorded conversations obtained with the prior consent of one party as follows:

(a) between Houston, Texas Police Chief Carrol M. Lynn and Joe Humbarger, Assistant Supervisor, Radio Technician, Houston, Texas Police Department. This is marked as *Exhibit 8(A)*.

(b) between Houston, Texas Police Chief Carrol M. Lynn and Lt. Joe Singleton, formerly with Criminal Intelligence, Houston, Texas Police Department. This is marked as *Exhibit 8(B)*.

(c) between Houston, Texas Police Chief Carrol M. Lynn and Radio Technician Charles Everts, Houston, Texas Police Department. This is marked as *Exhibit 8(C)*.

(d) between Houston, Texas Police Chief Carrol M. Lynn and Lt. J. D. Belcher, formerly with the Vice Division of the Houston, Texas Police Department. This is marked as *Exhibit 8(D)*.

(e) between Robert Tarrant, Criminal Defense Attorney, Houston, Texas, and Lt. Edward Kennedy, former lieutenant with the Narcotics Division and currently a lieutenant with the Communications Division, Houston, Texas Police Department. This is marked as *Exhibit 8(E)*.

(9) Excerpts from the transcript in *U.S. v. Dudley Clifford Bell, Jr.*, Criminal Number 72-H-361, United States District Court for the Southern District of Texas, Houston Division, which reflect statements made in open court by Mr. Richard DeGuerin, Attorney for the defendant, concerning the involvement of the Federal Bureau of Investigation in illegal electronic surveillance. This is marked as *Exhibit 9*.

(10) Letter from Houston, Texas Police Chief Carrol Lynn dated December 13, 1974, reflecting events in the F.B.I. investigation of the captioned matter which led to his conclusion that "I realized at this time that the whole investigation was a joke." This is marked as *Exhibit 10*.

(11) Memorandum from Captain B. G. Bond of the Houston, Texas Police Department dated December 13, 1974, reflecting in his opinion the unusual manner in which the F.B.I. conducted the captioned investigation. This is marked as *Exhibit 11*.

(12) Xeroxed copy of Federal Bureau of Investigation Report dated July 30, 1974, page one with synopsis, which indicates "no one has admitted having knowledge of any wire tapping aside from rumors." Subsequent investigative reports also reflect negative results. This is marked as *Exhibit 12*.

Numerous telephone calls and conferences with the Federal Bureau of Investigation, Houston, Texas, during which we expressed our concern and displeasure with the course of the investigation has resulted in no improvement. It is now apparent that further dilatory handling of this matter by the Federal Bureau of Investigation will result in loss of prosecutions by virtue of the *statute of limitations*. Therefore, it is imperative that we receive *immediate* investigative assistance from the Internal Revenue Service, Criminal Intelligence Division. Further reliance on the Federal Bureau of Investigation as the agency assigned jurisdiction in matters pertaining to Title 18, United States Code, Section 2510 et seq., in my opinion will be disastrous.

Accordingly, we respectfully urge the immediate designation of the Criminal Intelligence Division of the Internal Revenue Service, Houston, Texas, and specifically Agents I. A. Filer, Jack Hollingshead, Don Nettles and Frank Zapalac as the investigating authority for the captioned matter. As the bases for such an authorization we cite the following reasons:

(1) Vital experience and familiarity in directly related matters since June of 1971.

(2) Allegations of the possibility of participation of the local office of the F.B.I. in illegal electronic surveillance.

(3) Documented evidence as enclosed herewith of totally inadequate and unprofessional investigation by the Federal Bureau of Investigation, Houston, Texas.

(4) Documented evidence as enclosed herewith of partisanship between the Houston Police Department and the Federal Bureau of Investigation that has thwarted the investigation.

(5) Service to the interests of society and justice.

Furthermore, we request an immediate response to our request since each additional day of delay in investigation is resulting in a substantial detriment to the successful prosecution of this vital matter.

Very truly yours,

Anthony J. P. Farris,
United States Attorney

Enclosures as stated

MR. BLAKEY: Was there an answer to it?

MR. FARRIS: Not to me.

CHAIRMAN ERICKSON: So as far as you know, the letter has not been answered?

MR. FARRIS: Not to me.

MR. BLAKEY: Has your successor received an answer to it?

MR. FARRIS: I can't answer.

MR. BLAKEY: You do not know?

MR. FARRIS: I don't know, no, sir.

MR. BLAKEY: Will the staff see if his successor received an answer?

CHAIRMAN ERICKSON: Let the staff complete its examination.

MR. HERSHMAN: Will you summarize what you wrote to Attorney General Saxbe?

MR. FARRIS: I started with the heroin peddler who had been active for several years in Houston, and his conviction, the indictment of the nine officers, and sent as exhibits copies of the various letters and memos I had sent to the FBI SAC, Houston in this matter, and to his successor, because he retired in May of '74. And I continued to send this material to his successor because the investigation wasn't progressing. I sent all this material as exhibits to General Saxbe and asked for help.

MR. HERSHMAN: Mr. Farris, do you know why the FBI dragged its heels, as you say, in conducting this investigation?

MR. FARRIS: No, I don't. That they dragged their heels is apparent from the record, which I'm sure your staff has already investigated. Why they did it—I can only go back to the fact that there is this need for rapport between any FBI office and any local law enforcement office, be it the police department, be it the sheriff's office, the state police, whatever, because they do work together in many, many cases. So they do have to have a rapport, if you will.

Obviously, the investigation of a local law enforcement agency by the FBI is going to cause some hard feelings. And I have discussed this problem with brother U.S. Attorneys at length on many occasions, and we have agreed that if you are going to investigate a local law enforcement agency, for God's sake, don't do it with the local office FBI agents. Bring in agents from another office.

And we discussed this specific problem with Bill Cleveland of the FBI, five U.S. Attorneys and I, in December of 1973, that there was a great need for the FBI to bring in agents from another jurisdiction to investigate allegations of corruption, et cetera, of a police department. It fell on deaf ears. But I believe that is probably the case.

MR. HERSHMAN: Did you have any indication, sir, that perhaps they were reluctant to investigate the matter because it might involve federal complicity?

MR. FARRIS: I don't think so. I can question the fact that some of the FBI agents may not be the competent creatures that we have been led to believe in specific cases. But I have no reason to question their integrity.

As to allegations that FBI officers may have been involved in illegal wiretapping, I had no evidence presented to me that this was so. I had allegations; I had rumors. I read transcripts where defense counsel made those allegations. I sent those to the FBI.

So all I can say is that it had nothing to do, in my opinion, with any fear that their own were involved and so they would be reluctant to investigate.

MR. HERSHMAN: Why did you originally want the Internal Revenue Service agents to continue the investigations into illegal wiretapping?

MR. FARRIS: Well, they had more familiarity with the actors in the play. They had been investigating the Houston Police Department on the allegations of the rip-offs of some of these defendants, the allegations of the selling of narcotics by Houston Police Department officers—all, of course, leading to tax evasion.

And I felt that if they already had all of that in their dossiers that they were the most logical agency to continue. After all, they were already in it.

And I made the request formally to the IRS and got turned down.

MR. HERSHMAN: During your term in office, did you hand down any indictments for illegal wiretapping by Houston police officers?

MR. FARRIS: The nine that I mentioned earlier?

MR. HERSHMAN: Other than those nine.

MR. FARRIS: Other than those nine, no.

MR. HERSHMAN: Did you have allegations that other than those nine officers were involved in illegal wiretapping?

MR. FARRIS: Oh, yes. This is why I asked the SAC to investigate.

MR. HERSHMAN: Do you attribute your inability to bring forth specific findings on illegal police wiretapping to the so-called lack of cooperation by the FBI?

MR. FARRIS: I certainly do. After all, the U.S. Attorneys do not have investigators. We had to rely on the particular agency that was chartered by Congress to investigate that particular violation.

And I have seen the FBI make an all-out effort on cases that they consider important—hijackings, kidnappings, bank robberies, et cetera. I have seen them bring in agents from other jurisdictions to do this. I have seen them turn out the entire office for a case.

And it is rather incongruous that for this particular case, an investigation of the police department in the fifth largest city in the country, they made such a poor effort, and they couldn't put together a team of experienced agents from another area to bring them in and do it. They didn't.

MR. HERSHMAN: Thank you.

CHAIRMAN ERICKSON: Chief Andersen.

MR. ANDERSEN: I have no questions.

CHAIRMAN ERICKSON: Judge Shientag?

MS. SHIENTAG: No questions.

CHAIRMAN ERICKSON: Professor Blakey.

MR. BLAKEY: How long were you a United States attorney?

MR. FARRIS: About seven weeks short of six years, Professor.

MR. BLAKEY: And in that capacity, you had experience with what federal agencies?

MR. FARRIS: All of them—Secret Service, Customs, BNDD, Postal Inspectors, FBI.

MR. BLAKEY: I take it they would come to you with investigative problems?

MR. FARRIS: Yes.

MR. BLAKEY: For advice on legal aspects of investigations and to try them for them?

MR. FARRIS: Yes.

MR. BLAKEY: Did you ever have any other situations, apart from the one you have described today, where during the course of one investigation violations of another agency's statutes would come up? For example, during the course of the Secret Service investigation into counterfeiting, stolen bonds would come up that would fall within the FBI jurisdiction. Was that a common problem?

MR. FARRIS: Yes.

MR. BLAKEY: Did you find a reluctance in other agencies to pick up older investigations?

MR. FARRIS: No, never did.

MR. BLAKEY: Your testimony is that routinely other agencies, with no hesitancy at all, were willing to come in on a cold trail?

MR. FARRIS: If their policy did not forbid it, yes.

MR. BLAKEY: I am not asking you really for the policy. I said: Was there a reluctance?

MR. FARRIS: Not apparent to me.

MR. BLAKEY: I was in the Department of Justice less than—well, about the same time you were, and I found it a constant problem to get the FBI to investigate anything that had been begun by somebody else, or to get the IRS to investigate anything that had been begun by the FBI, or the Secret Service to investigate anything that had been done by the FBI, or for the FBI to investigate anything that had been done by the Secret Service. And frankly, I find your testimony here today that you didn't find that to be true, in light of my own experience—

MR. FARRIS: You didn't let me finish my answer, sir.

MR. BLAKEY: Be my guest.

MR. FARRIS: I found the FBI had reluctance to investigate matters that had already been investigated by other agencies.

MR. BLAKEY: Was this true not only in wire-tapping cases but in other areas?

MR. FARRIS: Yes. I did not find the reverse, the other agencies being reluctant to investigate cold trails.

MR. BLAKEY: If it is true that you found this to be the case in cases not involving police corruption, why do you attribute the reluctance in this case to a reluctance to follow police corruption rather than other—

MR. FARRIS: I don't understand the question.

MR. BLAKEY: It is your testimony that this investigation was not carried forth as you would have liked to have seen it.

MR. FARRIS: Yes.

MR. BLAKEY: It is your testimony that you attribute this to a reluctance on the part of the FBI to investigate local police.

MR. FARRIS: Yes.

MR. BLAKEY: You have also testified that you found a general reluctance on the part of the FBI to pick up any cold trail.

MR. FARRIS: That is correct.

MR. BLAKEY: Well, why do you attribute this case to reluctance to investigate the police as opposed to general reluctance to investigate cold trails?

MR. FARRIS: I think we are discussing apples and oranges here.

MR. BLAKEY: I thought we were discussing investigations.

MR. FARRIS: You are being facetious, Professor. I am talking about the fact in this particular

case, the investigation of the Houston Police Department, there was only one agency that could possibly investigate by charter, and that was the FBI. In other cases, we had instances where either agency could have investigated. There are cases where the ATF can investigate or the FBI can investigate. On wiretap matters, the charter is only the FBI's, which means if they didn't investigate it, it wasn't investigated.

MR. BLAKEY: Let me return to the question I asked you originally. Why do you attribute this particular reluctance in this case to an unwillingness to investigate the police department as opposed to a general unwillingness to follow cold trails? Do you understand the question?

MR. FARRIS: I understand the question. I thought I had already answered it.

MR. BLAKEY: You are drawing an invidious inference here based on the lack of investigation in this case and attributing it to a bad motive, when your testimony is they did this in other cases, when it is not related to a bad motive, but to an unwillingness to carry the responsibility for mistakes earlier made in the course of investigations.

I am trying to find why you attribute a bad motive to the Bureau in this case.

MR. FARRIS: Because that is the way I feel. I feel that they didn't want to investigate this case.

MR. BLAKEY: All right. What is the source of that feeling? Did you talk to the SAC?

MR. FARRIS: I talked to the SAC.

MR. BLAKEY: Did he say he was unwilling to do it?

MR. FARRIS: No, he was disinterested in the matter.

MR. BLAKEY: What did he say?

MR. FARRIS: He listened.

MR. BLAKEY: And said nothing?

MR. FARRIS: And said nothing.

MR. BLAKEY: And you inferred from this—how did you present the issue to him? In a dry, matter-of-fact way that I am hopefully asking you questions?

MR. FARRIS: Yes, that is correct.

MR. BLAKEY: And elicited no response whatsoever from him?

MR. FARRIS: None.

MR. BLAKEY: In your general relationships with him, was he this way?

MR. FARRIS: Yes.

MR. BLAKEY: Why would you then draw a bad inference in this case?

MR. FARRIS: The record speaks for itself, Professor. He had 100 agents to investigate a very complex case, and he assigned one.

MR. BLAKEY: Do you know what the case load of the Houston office is?

MR. FARRIS: I couldn't give you the statistics, but I know that—

MR. BLAKEY: Do you know what the case load of each of the officers in the Houston office was?

MR. FARRIS: No.

MR. BLAKEY: Are you prepared to testify here today that he had available to him manpower that he could have put on the case and did not?

MR. FARRIS: I have already testified, Professor, that in other cases, which in the SAC's opinion merited the priority—

MR. BLAKEY: Kidnapping?

MR. FARRIS: Kidnapping, hijacking, bank robberies.

MR. BLAKEY: Where a child's life was in danger he brought people in immediately. But I take it this was a trail that was two or three years old.

MR. FARRIS: Not necessarily.

MR. BLAKEY: He should have brought in 25 or 30 agents from outside the state to do the investigation.

MR. FARRIS: If he had had five agents, five seasoned, aggressive agents.

MR. BLAKEY: Do you know what his manpower situation was?

MR. FARRIS: I think I have testified that he had approximately 100 agents.

MR. BLAKEY: Do you know what they were doing at the time, what other cases they were assigned to?

MR. FARRIS: Among other things, they were investigating cases involving theft from interstate shipment, which to me was not as complex or as important as this particular case.

MR. BLAKEY: What we are getting into is a quarrel between priorities; right?

MR. FARRIS: Yes, that is correct.

MR. BLAKEY: Are you suggesting to us that they were not going to investigate this ever or simply they were not going to investigate it at your speed?

MR. FARRIS: Simply that they were not going to investigate it at my speed.

MR. BLAKEY: How long has this investigation been pending in the Department now?

MR. FARRIS: I don't know what you mean by "the Department," because the Department apparently hasn't done anything about it.

MR. BLAKEY: Well, from the first letter that you wrote asking a formal investigation up to now?

MR. FARRIS: Yes.

MR. BLAKEY: Approximately how long has it been?

MR. FARRIS: The first letter that I wrote that I sent the General Crime Section a copy of was April of 1974.

MR. BLAKEY: And now this is—

MR. FARRIS: —June of '75.

MR. BLAKEY: June of '75. And what is the statute of limitations on these offenses?

MR. FARRIS: Five years.

MR. BLAKEY: Assuming they occurred in the last two or three years, I take it they still have plenty of time before the statute runs, haven't they?

MR. FARRIS: Sure, and they have also lost several cases where the statute has run out.

MR. BLAKEY: Mr. Farris, if I understand your testimony, it is not that they have not and will not do anything; it is that they have not done it yet and have not done it with the speed that would suit you; is that correct?

MR. FARRIS: Not quite. They had not done it as of the time that I left office. I cannot speak since December 30 of '74.

MR. BLAKEY: If tomorrow indictments were returned against 25 or 30 officers, would you feel that you ought to reconsider your testimony?

MR. FARRIS: No, I would say that perhaps my prodding in my letter of December 17, 1974, had something to do with it.

MR. BLAKEY: Would you believe someone else was a reasonable person if he drew the conclusion that your complaint made no difference in any way, that the Bureau did what it does in all cases—pursue its cases in its own way in its own time; and no amount of prodding on the part of the Department of Justice gets the Bureau to do things in the Department's way as opposed to the Bureau's way but eventually they will get to it and get it done?

MR. FARRIS: Hopefully.

CHAIRMAN ERICKSON: Are you through, Professor Blakey?

MR. BLAKEY: Yes, sir. Thank you.

CHAIRMAN ERICKSON: Mr. Farris, as a U.S. Attorney, one of your duties was to supervise the grand jury?

MR. FARRIS: Yes, sir.

CHAIRMAN ERICKSON: And was any of the material that was presented to you presented to a grand jury?

MR. FARRIS: Actually, very little since we had no investigators of our own. We presented witnesses that we had come up with through people calling us—by "people" I am talking about citizens—witnesses whose names we had secured from Chief Lynn, and some of the employees of the Southwest Bell Telephone Company.

CHAIRMAN ERICKSON: Did Chief Lynn cooperate with you?

MR. FARRIS: Yes.

CHAIRMAN ERICKSON: Did he give you all the information you requested?

MR. FARRIS: He gave us all he had.

CHAIRMAN ERICKSON: And was the information such that it had the names of the so-called offending federal agents included?

MR. FARRIS: I can't go into that because I was in the grand jury room when some of that was presented, and I would be violating Rule 6(e).

CHAIRMAN ERICKSON: I am very well aware of the rule.

MR. FARRIS: I know you are, Judge.

CHAIRMAN ERICKSON: I am only inquiring whether the names were provided. I am not asking what the names were. I am just asking—

MR. FARRIS: Leads were provided, let me say that.

CHAIRMAN ERICKSON: Well, there is quite a difference between leads—we have been given a pretty good lead that all wasn't well in the Houston Police Department, but if I were to have to name the officer that violated Title III, I'd have a very difficult time doing it from the testimony that I have.

What I am asking is: Were you given the names of the federal agents that supposedly walked in when the illegal wiretap was being conducted by the Houston Police or by the BNDD or the DEA, whatever you want to call it? Both of them were supposedly aware of what the Houston police were doing.

MR. FARRIS: Yes, we were.

CHAIRMAN ERICKSON: And you provided those to the Attorney General?

MR. FARRIS: That is correct.

CHAIRMAN ERICKSON: And your letter of December 1974 requested action?

MR. FARRIS: Yes, sir.

CHAIRMAN ERICKSON: And nothing occurred prior to the time you left office?

MR. FARRIS: That is correct.

CHAIRMAN ERICKSON: After you talked to the special agent in charge of the Houston office, did you at any time request a status report?

MR. FARRIS: Constantly.

CHAIRMAN ERICKSON: And what was the response?

MR. FARRIS: The response was one of lack of concern—minimal response.

CHAIRMAN ERICKSON: As old trial lawyers, we probably have a tendency to get the cart before the horse. That is a conclusion, isn't it?

MR. FARRIS: Yes, sir.

CHAIRMAN ERICKSON: What did he say?

MR. FARRIS: That they were doing the best they could, and the reports were forthcoming. And as I have already stated, the reports weren't good enough to present to the grand jury.

CHAIRMAN ERICKSON: The reports that were presented to you did not contain the meat, as you put it, that would enable a grand jury to take action.

MR. FARRIS: Yes, sir, that is correct.

CHAIRMAN ERICKSON: You had the names of the actual officers on the Houston Police Department that were provided to you by the Chief of Police?

MR. FARRIS: Some of them.

CHAIRMAN ERICKSON: And you turned over the information that you obtained from the Chief of Police to the FBI?

MR. FARRIS: Yes, sir.

CHAIRMAN ERICKSON: Did this question of the inner working between the Federal Bureau of Investigation and the Houston Police Department come into play, the fact that they did work together on cases?

MR. FARRIS: Well, it was apparent all the time I was in office that they worked together. They had to work together. There were many cases that were, if you will, interlocking cases.

CHAIRMAN ERICKSON: Well, from your experience, there were many narcotics cases in which it would be a joint effort of the Houston Police Department and the FBI?

MR. FARRIS: And the DEA on narcotics.

CHAIRMAN ERICKSON: And on other crimes?

MR. FARRIS: Yes.

CHAIRMAN ERICKSON: Was any effort made to determine or investigate the taps that were placed on the phone of the Chief of Police, Chief Lynn?

MR. FARRIS: You mean by the FBI?

CHAIRMAN ERICKSON: Yes. Or was that information turned over to them as well?

MR. FARRIS: Chief Lynn personally visited with the SAC.

CHAIRMAN ERICKSON: Were you there?

MR. FARRIS: No, sir. And subsequently the Chief was visited by a couple of FBI agents and a couple of people from the Southwestern Bell Telephone Company who checked his phone.

CHAIRMAN ERICKSON: So as I understand it, your belief is that if we are going to cause Title III to be enforced, it would be effective to have the enforcement tool turned over to an investigative unit other than the FBI.

MR. FARRIS: No, no, no, no. I don't want to leave this Commission with the idea that I am critical of the FBI generally, or even critical of the FBI in Houston generally. I am critical of the Houston office of the FBI in one case—which isn't bad for six years—in one case, this case.

I don't question the FBI's ability or manpower resources or scientific know-how to investigate most anything that they are chartered to do. What I am saying is that if it deals with local law enforcement entities that it should not be handled by the guys who have to deal with them from the FBI office on a daily basis.

CHAIRMAN ERICKSON: May I conclude from that, that what you are suggesting is that they ought to have a regulation within the Department, or there should be a means of directing that investigations be carried on by other than the local office of the FBI.

MR. FARRIS: That is correct.

CHAIRMAN ERICKSON: That is your recommendation?

MR. FARRIS: Yes, sir.

CHAIRMAN ERICKSON: You think the FBI is competent and probably the agency that should do the investigating, but that it should not be permitted by the local office that works with the group that, in effect, is being investigated.

MR. FARRIS: That is substantially it.

CHAIRMAN ERICKSON: You had one further question, Professor.

MR. BLAKEY: Well, it may turn out to be more than one, Mr. Chairman.

CHAIRMAN ERICKSON: I wouldn't be surprised.

MR. BLAKEY: How many assistants did you have assigned to you?

MR. FARRIS: Thirty-two.

MR. BLAKEY: How many grand juries did you have available to you?

MR. FARRIS: One in each division. I had six divisions.

MR. BLAKEY: Could you ask for more from the chief judge?

MR. FARRIS: The only way I could have had more, I think, would have been a special grand jury, and I would have had to have permission from the chief judge.

MR. BLAKEY: You could have gotten it if you really needed it?

MR. FARRIS: I think that during a certain period of time I actually had a special grand jury in session so that I probably would have been turned down by the chief judge on a second grand jury.

MR. BLAKEY: How many assistants did you have assigned to this investigation?

MR. FARRIS: I started out with the Assistant Chief of the Criminal Division, and I believe I worked it up to four. And when you consider that is one-fourth of the criminal division in the office, that is quite an effort.

MR. BLAKEY: Did they have subpoena power available to them?

MR. FARRIS: Yes, sir.

MR. BLAKEY: Why didn't they do an investigation on their own if you were dissatisfied with the Bureau?

MR. FARRIS: We did. We subpoenaed several officers before the grand jury in Houston.

MR. BLAKEY: And that wasn't satisfactory to you?

You can see as well as I can the point I am making. I was in the Department for a considerable period of time, and if we didn't like what the Bureau did for us we did it ourselves. Sometimes it was a little harder, but if we put a priority on it and thought it was important, and the Bureau didn't share our priority, we put our own people on it.

What I am trying to ask you is this: if you thought this was that much more important than the SAC did, and you had lawyer power available to you, you had grand jury power available to you, why didn't you run the whole case out yourself?

MR. FARRIS: To answer your question, I did end up assigning one-fourth of the Criminal Division to this case. We did investigate it. We did subpoena various officers and other individuals. And I can not tell you what they said or even tell you whether they said it, obviously.

MR. BLAKEY: Did you secure any indictments?

MR. FARRIS: We didn't get the names until November of '74.

MR. BLAKEY: So you had done the best you could just before you left?

MR. FARRIS: That is correct.

MR. BLAKEY: Should someone criticize you for not having done more while you were there?

MR. FARRIS: I don't see why not. When you are in a job like that, you expect criticism and you take the—

MR. BLAKEY: Some good and some bad.

MR. FARRIS: Sure.

MR. BLAKEY: Thanks.

MR. FARRIS: I have some suggested changes for the existing law, Mr. Chairman.

CHAIRMAN ERICKSON: I would be delighted to hear those.

MR. FARRIS: One of the first problems is there are no misdemeanor provisions in the law—none. So if you are trying to make a case, you have a choice of giving a man immunity—completely giving him immunity and he gets away with whatever he has done, or you don't get his testimony, you don't get the higher-ups. You have no provision to say to him, "We will have you plead to a misdemeanor and let it be known to the judge that you have cooperated, and that is far better than a felony conviction."

I said "we." I keep forgetting I am a private lawyer now.

My former associates, the U.S. Attorneys, desperately need a misdemeanor provision in this law.

I also feel that the section on the manufacturers, 2512, is very inadequate. It is like a big piece of cheese full of holes. I think that the section should be rewritten to provide for licensing of the manufacturers, for the provision of having all the devices that the manufacturer—having serial numbers on them, record-keeping to make it imperative that they inform the Federal Government who they sold the devices to. And every time the devices change hands, that has to be reported.

I have already heard testimony here today that there are more devices that are sold to law enforcement people and private eyes, and so forth, in states that do not have enabling legislation than to the ones that can use it legally. And it is going to get worse if the section is not changed to provide, as I say, for very stiff licensing.

And I have talked to some of my friends who are still U.S. Attorneys, and they feel that there is a very strong need to provide for this. And if the Commission doesn't recommend it, it will be worse next year, and the year thereafter.

CHAIRMAN ERICKSON: May I inquire whether, with all due deference to the draftsman of the bill, you find this bill is somewhat complex and difficult to understand and difficult to follow?

MR. FARRIS: You mean as presently written?

CHAIRMAN ERICKSON: Yes.

MR. FARRIS: Not that complex. There are some prosecutors who feel that the definition of "wire communication" is not clear enough. They feel that they sometimes do not know whether to prosecute a husband tapping his wife or the reverse.

But basically, as it is written, it is merely inadequate, rather than complex.

CHAIRMAN ERICKSON: You think that amendments are needed to plug up some of these holes in the Swiss cheese, as you say.

MR. FARRIS: Yes, sir. And I think that the portion allowing the telephone company and others to—I think the quaint word is "monitor" telephones—I have to agree with one of my friends who is a U.S. Attorney, that there must have been heavy lobbying by the telephone system to get that in there.

When you have, as for example, I heard of a case out in California—I think it was Macy's—where they were tapping their employees' phones, and the judge read the section and said it was not a violation.

Well, I think it's a violation. I can see the telephone company monitoring subscribers' phones to find out if they are using blue boxes, to find out

if they are cheating on the telephone company, but I have a problem understanding who monitors the monitors. What background investigation did AT&T have on these people who sit there in these little rooms listening to telephone conversations of people who pay the telephone bill? I have a problem with that, and so do my former associates who are U.S. Attorneys.

And I think the portion of the law that this judge in California had trouble with should be clarified so that a judge and, in fact, a prosecutor can tell whether, in fact, a businessman should be prosecuted for listening in to his own employees to see if they are lazy or incompetent or stealing from him. I think that ought to be tightened up.

That's about the sum of my recommendations.

CHAIRMAN ERICKSON: Thank you for coming. We appreciate what you have done for us. I hope we can reach some of the ends that you see as necessary adjuncts to the proper use of this for law enforcement purposes and to protect privacy.

Your prepared statement will be included in the record.

[The statement of Anthony J. P. Farris before a House subcommittee, together with other relevant materials, follows.]

Washington, D.C.
May 22, 1975

Prepared Statement of Anthony J. P. Farris,
Former United States Attorney for the Southern
District of Texas, Before the Subcommittee on
Courts, Civil Liberties and the Administration of
Justice of the House Judiciary Committee

MR. CHAIRMAN: My name is Anthony J. P. Farris, and I am an attorney with Farris, Pain & Horne in Houston. From February 14, 1969, to December 30, 1974, I served as United States Attorney for the Southern District of Texas, with the principal office in Houston. The District is the eighth largest of the 94, and Houston is the fifth largest city in the country.

During my tenure, my office had the following successful prosecutorial record: 1969 through 1974, a 98.630 successful percentage for the six years; brought more successful civil and criminal pollution litigation (principally under the Refuse Act of 1899) than all my predecessors put together; increased the collection efforts of the office from a low of \$445,303.00 to a high of \$2,036,865.00 for a six year total of \$7,994,427.00; remained in the top five in total narcotics prosecutions for six years and was first one year; more active civil rights cases than all my predecessors; and handled diverse and complicated civil cases successfully. All this in spite of a *higher* case load per lawyer than *all* the seven offices, larger in size, than Houston. I also hired more minorities than all my predecessors put together.

I give you the above facts and figures, *all* being of record and all easy to *check*, because of the importance of your Committee—also, I may not have another such opportunity. The above *very successful* record was put together with a staff that reached a peak of 32 lawyers, with at least 20 having no previous experience when they joined the office. Mr. Chairman, I long have resented hearing and reading remarks attributed to Federal

Judges from the District Court to the Supreme Court level, to corporation lawyers in the ABA, and to Members of both Houses of Congress, questioning the ability of these fine young men and women. Many of these fine young lawyers, in every judicial district, consistently take the measure of some of the best criminal defense lawyers and some of the best big firm lawyers in the country. I might also add that *most* of the critics have never, repeat never, tried a criminal case on either side of the docket. Thank you for allowing me the time to get that off my chest.

I understand I am here to testify about allegations of illegal wiretapping by law enforcement authorities in Houston, Texas, about allegations of illegal wiretapping by federal authorities in Houston, and about the degree of aggressiveness in investigating and prosecuting these alleged violations.

First, tax evasion investigations in these matters were commenced by the I.R.S. in 1971 and culminated in the conviction of Sebastian Mirelez, an alleged big-time heroin dealer in Houston. Further investigation resulted in the conviction of a former Houston Police Department officer for perjury. Continuing investigation by the I.R.S. resulted in the indictments of nine H.P.D. officers on charges ranging from income tax evasion, sale of heroin, and civil rights violations, to illegal wiretapping. *This* investigation started in December, 1972. The indictments were returned May 31, 1974. This case is pending. Obviously, I am limited on what I can say.

The very thorough investigation by the I.R.S. led to the conclusion that *other* H.P.D. officers could have been involved in illegal wiretapping. I asked the I.R.S. Criminal Intelligence Agents to *continue* the *already* ongoing probe as to the wiretapping. The agents declined, informing me that Commissioner Alexander would permit them to conduct *only* Title 26 investigations. And so, although they were already well acquainted with the case, they could not go on. We discussed the matter, orally, with the F.B.I. in Houston, and finally, in April, 1974, asked them in writing (with a copy to the General Crimes Section of the Criminal Division of the U.S. Department of Justice) to commence (if they had not already done so) a comprehensive investigation of the alleged wide-spread illegal wiretapping by the H.P.D.

Concurrently, of course, my office commenced an investigation by Grand Jury. I personally participated in some of those sessions of the Federal Grand Jury in Houston. Under the Federal Rules of Criminal Procedure, Title 18 U.S.C.A., Rule 6(e), I am limited by the rules of secrecy as to what I can discuss. I am likewise limited by Rule 3 of the Local Rules of the United States District Court for the Southern District of Texas, which deals with Release of Information by Attorneys, and specifically Section "A" in Criminal Cases and Section "B" in Grand Jury Proceedings. Last, but not least, I am also limited by Title 5, U.S.C., Section 522(6)(7) on the disclosure of files and information compiled for law enforcement purposes and the regulations implementing that section, and Title 28, Code of Federal Regulations, Sections 16.21-16.26 on disclosures by both employees and former employees of the U.S. Department of Justice.

On the matter of the allegations of illegal wiretapping by federal agencies, there is little I can say. I read and heard various charges made that D.E.A. Agents allegedly participated in illegal wiretapping. To a much lesser extent, I read and heard the same allegations about F.B.I. Agents. I neither saw nor read any evidence, soft or hard, to support those charges. No one came forward to testify or to document those charges while I was in office.

My real main concerns have been that the investigation of the H.P.D. has lasted so long and has effected some 2,300 officers when at *the most* some 50 were allegedly involved. Finally, I feel that the investigations in *this* case as conducted by the Houston office of the F.B.I. up to December 30, 1974, were less than thorough, less than aggressive, less than comprehensive, and less than enthusiastic.

FARRIS, PAIN & HORNE

ATTORNEYS

2 HOUSTON CENTER

909 FANNIN

HOUSTON, TEXAS 77002

SUITE 1016

(713) 654-4437

May 19, 1975

Mr. Kenneth J. Hodson, Executive Director
National Commission for the Review of Federal and State Laws
Relating to Wiretapping and Electronic Surveillance
1875 Connecticut Avenue, N.W.
Washington, D.C. 20009

Dear Mr. Hodson:

I am in receipt of your letter of May 9, 1975, inviting me to testify at the hearings of the Commission sometime around June 25-27, 1975. As I understand, this would be concerning the effectiveness of Sections 2511 and 2512 of Title 18 U.S.C.

Please find enclosed a short biographical outline on me as well as a copy of the prepared statement, and a letter of transmittal sent to Mr. Bruce Lehman, Counsel to the House Judiciary Committee. As you will note by said letter of transmittal, I am appearing before Congressman Kastenmier's Subcommittee on May 22.

In answer to your four questions:

(1) I found problems in prosecuting cases of illegal electronic surveillance under the current Federal statutes in those instances where the cases involved family squabbles, attempts to catch dishonest employees, and cases of that type. Difficulties were in not having the manpower to prosecute cases of that type which would mean letting more important cases just sit. In that particular type of case, therefore, we sometimes deferred prosecution.

(2) As to the difficulty in interpreting the statutes, there was really no difficulty in interpreting Section 2511, but it is my understanding that some District *Judges* have had difficulty interpreting it. Such as the District Judge deciding that a "self-contained" telephone system fell within the exception specified in (2) (a) (i) of 2511. I think most U.S. Attorneys would interpret the statute as merely permitting telephone companies to monitor telephone equipment-functioning, and *nothing more*. Perhaps Congress could be more specific in detailing the wording in reference to the exceptions.

As to 2512, I think here there are many questions about such things as when can a "device" be assembled and sold, when can it be sold disassembled, who are the exempted agencies, and what constitutes a contract between a manufacturer of this device and an exempted agency

(3) Please see my prepared statement for the Judiciary Subcommittee on Question 3.

(4) Please see my prepared statement to the Subcommittee on Question 4

I would appreciate your advising Ms. Elizabeth McCulley of your staff that I will require hotel accommodations during my stay in Washington so that she may secure government rates.

Very truly yours,

[Signed] Anthony J. P. Farris

AJPF/ssb

Enclosures

FARRIS, PAIN & HORNE

ATTORNEYS

2 HOUSTON CENTER

909 FANNIN

HOUSTON, TEXAS 77002

Suite 1016

(713) 654-4437

June 27, 1975

Honorable William H. Erickson

Chairman, National Commission for the Review
of Federal and State Laws Relating to

Wiretapping and Electronic Surveillance

1875 Connecticut Avenue, N.W.

Washington, D.C. 20009

Dear Judge Erickson:

I refer to my testimony before the National Commission on June 25, 1975. Unfortunately, so much time was spent on "the Houston story" that not enough time remained to discuss possible changes in the present statutes. I am taking the liberty of writing this letter to "flesh" out my recommendations and to expand somewhat on those I made orally.

Section 2510

I. "Wire communication" indicates that the interception of a radio-telephone communication is an interception of a "wire" communication, but this is not clear enough. **RECOMMENDATION:** Make this definition clear and spell it out.

II. "Person" does not spell out whether "person" is or is not "empowered by law" (of his or her state) to intercept wire or oral communications. **RECOMMENDATION:** Make it clear and spell out that "person" is not so empowered by said (necessary) state enabling legislation.

III. "Investigative or law enforcement officer" is not clear on the point that in addition to being "empowered by law" to conduct investigations . . . these officers are also empowered by (state) law to make legal interceptions of wire and oral communications. **RECOMMENDATION:** Make it clear and spell out that these people are the ones who are so authorized.

IV. "Communications carrier" is not clear on whether that includes switchboard operators or security guards at Macy's in San Francisco in addition to the AT&T people. **RECOMMENDATIONS:** This should be nailed down to mean the Bell System, General Telephone, Western Union, etc., and not Macy's, not Bank of America, not General Electric, and not Maw and Pa's Emporium in Topeka, Kansas.

Section 2511

(1) Here you should nail down that only those Federal Agents authorized by statute and only those state "investigative or law enforcement" officers authorized by enabling legislation passed in their individual states are exempt.

(2)(a)(i) and (ii) These provisions should be re-written so that while still permitting the carriers the latitude to ferret out blue box users and others who steal service as well as to monitor for faulty equipment would, at the same time, have strict guidelines as to when the monitoring was permitted, which (screened) personnel were to do it, have the non-random provision repeated, forbid the monitoring procedure for other purposes, and clearly spell out that other business entities, i.e., Gimbel's, General Motors, Old Colony Trust, Pat & Max's Dry Goods Store in Cut and Shoot, Texas, etc., were prohibited to monitor their lazy, stupid, incompetent, dishonest or immoral employees as well as forbid "wiring up" elevators and public places to hear customers' conversations.

A new subsection needs to be added to Section 2511 to make it a violation to fail to notify the proper authorities that a principal has violated the provisions of this chapter. (Example: An

investigative or law officer, State or Federal, standing by watching an illegal interception and doing nothing about it, or being told about an illegal interception and doing nothing about it, such as has been alleged both in Houston, Texas, and Williamsport, Pennsylvania.) A second part of the subsection might provide for written notification to be made to both the FBI and the United States Department of Justice in Washington, D. C.

P.S. 18 U.S.C. §4, Misprision of Felony, is inadequate. According to *Lancey v. U.S.*, CA, Cal. 1966, 356 F2d 407 (cert. denied) and *U.S. v. Daddano*, CA, Ill. 1970, 432 F2d 1119 (cert. denied), the Government must prove that Defendant "took affirmative steps to conceal the crime of the principal." If an Assistant United States Attorney has to prove that additional element, i.e., that the Agent or Policeman affirmatively took steps to conceal it, that places too much of a burden on the prosecutor and leaves a gaping hole for those agents/officers who just do not want to report it.

Section 2512

I feel that the only answer to the sale of wiretapping devices, bugging devices, or any devices which are designed for surreptitious use is to (1) license the manufacturers, (2) make them put serial numbers on all equipment (not too miniscule as to make it physically impossible), and (3) report all sales, trade-ins, leases, etc., to the United States Department of Justice, and make it clear that sale to law enforcement officials or "persons" in those states that did not pass enabling legislation is strictly "malum in se" with an exceedingly high fine for such violation. The Commission already has evidence of the large volume of sales made by manufacturers, etc., to "persons" in states where no enabling legislation has been passed—in violation of the law as presently written and with knowledge that they are violating the law.

Section 2518

8(a) Provides that: The contents of any wire . . . shall, if possible, be recorded . . . **RECOMMENDATION:** Make the recording portion MANDATORY with the proviso that if the equipment malfunctions, the portion of the overheard conversation may be admitted into evidence if two agents/officers can corroborate the contents of that portion not recorded.

(9) Provides that "the contents of any intercepted . . . or evidence . . . shall not be received in evidence . . . unless each party not less than ten days before the trial . . . has been furnished with a copy of . . . This ten-day period may be waived by the judge . . ." This subsection is quickly going to run head-on into the "Speedy Trial" provisions recently passed by Congress (as are the lack of enough judges and prosecutors not being provided by Congress). **RECOMMENDATION:** Eliminate the authority of the judge to waive the ten-day period. *Period.*

ADDENDUM

Tactically, prosecutions are handicapped by the LACK OF MISDEMEANOR provisions in this chapter. Prosecutors are often unable to obtain the cooperation of persons less culpably involved in the crime because the prosecutors either have to give those persons full immunity or charge them with a felony.

A misdemeanor provision needs to be added BUT not as a substitute.

Judge Erickson, I respectfully request that you and the National Commission make this letter a part of the record of these hearings.

Sincerely,

[Signed] Anthony J. P. Farris

AJPF/ssb

cc: Honorable Kenneth J. Hodson

Executive Director

National Commission for the Review of

Federal and State Laws Relating to

RECORD OF INTERVIEW WITH CAROL VANCE,
DISTRICT ATTORNEY OF HARRIS COUNTY
(HOUSTON), TEXAS, CONDUCTED JULY 25, 1975, AT
WASHINGTON, D. C., BY KENNETH J. HODSON AND
MICHAEL HERSHMAN OF THE STAFF OF THE NATIONAL
COMMISSION FOR THE REVIEW OF FEDERAL AND
STATE LAWS RELATING TO WIRETAPPING AND
ELECTRONIC SURVEILLANCE

HODSON: Mr. Vance, we would like to get your general background. To start with, how long have you been District Attorney?

HERSHMAN: I'd just like to note that the interview is being taped with the consent of all parties.

VANCE and HODSON: Certainly. Right.

VANCE: I've been in the District Attorney's Office in Harris County for 18 years, and I've been District Attorney there nearly 10 years now, or nine and a half years.

HODSON: And that's an elective office?

VANCE: Yes. It's an elective office. It's for Harris County, which includes numerous cities, the largest of which is Houston.

HODSON: About how big a staff do you have?

VANCE: We have 109 Assistant District Attorneys on the staff; we have a little over 200 people altogether.

HODSON: What are your relations with the Houston Police Department?

VANCE: Our relationship has been very close through the years. The police come to us constantly seeking advice on search warrants and warrants of arrest. We have an organized crime division, which we call the Special Crimes Bureau, which works with all law enforcement agencies including the Houston Police Department. Although we are completely independent agencies and make our judgments independent of each other, we have had a close working relationship with the Houston Police. They provide us perhaps 65 percent of all of our cases in that they cover perhaps 1.2 or 1.3 million people out of a county that is approximately 2 million in size.

HODSON: About 65 percent. Do you have a liaison man with them? Do they have a liaison man with you on a full-time basis?

VANCE: No. We do keep people over at the Police Department, but it is really our own office that they furnished us, that we call an intake division. We've had an office over there for about two years now that operates seven days a week, 24 hours a day. But, really, the kind of cases that we would work closely with them on, such as, say, a burglary ring, a narcotics ring, something of that nature—detectives out of those divisions would in all probability come to our Special Crimes Bureau and work directly with them on any particular facet of any type of organized criminal activity.

HODSON: Do you know the former Chief of Police of Houston, Carrol Lynn?

VANCE: Yes, I've known him for a good number of years, when he was a detective in homicide, when he was in charge of the Police Academy, and then, of course, as Chief of Police of Houston.

HODSON: During his testimony before the Commission on the 25th of June of 1975, then-Chief Lynn testified that information he had received indicated that there was widespread wiretapping going on in the Houston Police Department; that it had probably been going on for about 10 years; that it was conducted with the knowledge of at least some agents of the FBI; that it was done with the knowledge of the security office of

Southwest Bell; and that he considered that it was a very serious problem. He indicated that he had discussed it with the U.S. Attorney in Houston, and also had discussed it with you. He testified that he had had several long discussions with you about this; that you had prosecuted two policemen for wiretapping, back in 1973 before he became the Chief; that he had talked with you with respect to these matters; that he felt that you had faced a lot of heat from the Houston Police Department because you had prosecuted these policemen; and that you were not going to involve yourself in the internal workings of the Houston Police Department unless he could bring you some concrete evidence. Now that basically was his evidence on the 25th of June, and I'd like to have your comments with respect to those matters.

VANCE: Well, I would be very shocked if there were any widespread wiretapping because, concerning wiretapping or any allegations of wiretapping done by the Houston Police Department or by the FBI, or anyone as far as that goes, we've had a close working relationship with all the law enforcement agencies, including the Federal agencies, and the first time that we had had any allegations come to us of any wiretapping were the two Houston Police Department officers who had previously been indicted. They were indicted on a conspiracy to sell marijuana. Their names were Carlos Avila and Tony Zavala. They came to us and told us that there had been a lot of wiretapping going on by the Narcotics Division of the Houston Police Department. This was around April or May of 1973 that they were indicted, and then what happened was—actually the case was made by the Houston Police Department—that their attorneys came to us and they wanted to get them out of the case, so to speak, in return for their testimony to try to indict other officers. This was the first time we'd ever had any allegations of wiretapping. Since all of this has occurred, I've talked to everyone on my staff who might have any possibility of knowing about any wiretapping and, to a person, no one on the staff to this good day, to my knowledge, has known of any single case of wiretapping other than what people—what these two people—have told us except for hearsay upon hearsay perhaps that we have read in the newspapers. We have also read the testimony that had been given by the Chief of Police and others. We would not really investigate a wiretapping case, per se, in that we do not have any wiretapping statute; nor do we have any statute in Texas that makes it illegal to wiretap. We need a wiretapping statute as authorized by the Federal law very badly to fight organized crime, but we do not have that.

HODSON: You can't even prosecute them for, say, trespass?

VANCE: That's right. That's right. Well, trespass would be some type of city offense prosecuted over in the City Court that wouldn't carry over a \$200 fine. We would, of course, like to know of any specific cases in which any testimony was obtained pursuant to wiretaps, because we would be under an obligation to turn this information over to the court and to the defense attorney in the case. I knew that Chief Lynn had been conducting an investigation for some time and had testified about wiretapping by the police, and I wrote him a letter and asked him for any specific evidence that he had pertaining to any cases. I brought a copy of my letter to him, which is dated May 20, 1975, and then his reply some 10 days later on May 30, 1975, and I will leave these two copies to accompany the transcript.

HODSON: We will enter them as part of the record of this interview.

VANCE: Of course, the letters speak for themselves; but, in essence, Chief Lynn said that he had no such evidence of any wiretapping on any specific cases. Now, when this information was brought to us, we took action on one or two cases. I've brought some notes with me that have been prepared by the head of the Special Crimes Bureau, which actually participated in Avila/Zavala negotiations. They were given probation and they did testify and we did indict some other officers pursuant to

a scheme that was generally established by their testimony. This had nothing to do with wiretapping.

HODSON: Nothing to do with wiretapping?

VANCE: No, but these officers claimed that, instead of setting up physical surveillance for several days to get the probable cause type of information for search warrants, they took a short cut and wiretapped and found out about it, and then obtained the search warrant on the basis of the wiretap. Then they would doctor up the offense reports to make it appear that surveillance had been done for a number of days of seeing known buyers and sellers of narcotics addicts come and go.

HERSHMAN: Aren't these the same two officers who recently pleaded guilty before a Federal court to illegal wiretapping?

VANCE: Well, I think they have.

HODSON: Is that Avila and Zavala?

VANCE: Yes. And I think that if the government does anything with those cases, those two would be a couple of their key witnesses.

HERSHMAN: It's my understanding that these two officers, within the last two weeks, pleaded guilty to counts of wiretapping, and other counts of illegal activity involving narcotics were dropped. So that it was a form of plea bargaining for their testimony.

VANCE: That's my very definite impression, although I have no firsthand knowledge of that. All I know about that is what I have read in the paper and heard. These two officers were instrumental in our obtaining indictments, not only on wiretapping charges, but on other illegal activity. What was alleged was generally that certain people on the narcotics division—about six or seven of them—would find out that a certain load of heroin would be coming in, or something of this nature, and one person would have maybe \$10,000 to make the buy; they would make the buy and make the arrest, and then skim off maybe \$5,000 and turn over \$5,000 for evidence; they might even keep back part of the heroin to use for other informers. That was the general allegation, and we checked it out and believed it, and actually a couple of indictments were obtained on two police officers. They were both acquitted. The case had a full trial. I never felt any heat as Chief Lynn says. I would take issue with his statement. I certainly didn't feel any pressure on the part of the police or the former Chief or anybody else in the city not to investigate it, or anything of that nature. We investigated it and took it as far as we could. The only other thing that we did, acting upon this information, was to dismiss a couple of cases. There were two separate cases that were dismissed on the basis of what Avila and Zavala had said. We had no other evidence other than that they had said that there was wiretapping. But they did mention these two specific cases. Avila and Zavala were real vague when it came to naming names. They'd tell you how it was done, but they were real vague when it came to naming names so far as wiretapping went.

HERSHMAN: Are you suggesting that what they did was use information allegedly obtained from a confidential informant, when in reality it was a wiretap?

VANCE: That was what Avila and Zavala said. I don't know. I don't know to this day. They said that they were getting their information from wiretapping, but of course Avila and Zavala were trying to save their own necks because they had been indicted on an air-tight case as a result of an investigation by the Houston Police Department.

HODSON: An air-tight case of wiretapping?

VANCE: No. It was not wiretapping, it was a conspiracy to sell marijuana. They were actually involved in a marijuana transaction with a big marijuana seller.

HODSON: Why did they start talking about wiretapping when they were indicted for a non-wiretapping matter?

VANCE: Because the Police Department had investigated them, made this case on them, brought it to us, and sought an indictment. They were indicted and they were bitter towards the

Police Department as a result of this. And also they wanted to get out. If we tried the case on these two officers to a jury, I do believe they would have gone to the penitentiary for a long term of years, because it was a case where they were involved in a conspiracy to sell marijuana. First of all, they wanted dismissals and all this type of thing. We later did recommend that they received probation. We didn't promise them anything, but they knew that we would consider the fact that they had brought us this other testimony against these other officers, so later they did receive probation on a plea of guilty.

HERSHMAN: Were Avila's allegations of illegal wiretapping ever communicated to Federal authorities?

VANCE: Yes, they were. When they first brought this information to us—and my people were having discussions with them directly and also with their attorneys, Bob Turner and Bill Green—I personally called Tom Jordan, who was Agent-in-Charge of the FBI at that time and told him that we had some information we wanted to pass on to them, and I sent Bob Bennett, who heads my Special Crimes Bureau, and one or two other attorneys, over to his office. They sat down and told the FBI what the information was. As to what the FBI did with it from there, I just don't know.

HERSHMAN: You had no feed back?

VANCE: No. We had no feed back. But I didn't necessarily expect any because we had no information. All we had were these allegations—everybody's doing it—well, not everybody. Their allegations were limited to the narcotics division. Many people in the narcotics division are doing—that type of thing.

HODSON: About what date did you turn this information over to the FBI?

VANCE: Well, it was on . . . I have it here. I asked Bob Bennett to prepare a chronology of events so that I might answer these questions because a lot of time has gone by. July 3 is what he has down.

HODSON: What year?

VANCE: 1973. That was when Bob Bennett and two of his assistants personally visited Tom Jordan, Special Agent-in-Charge of the Houston Field Office of the FBI, and advised him that the two attorneys of Avila and Zavala had made allegations of illegal wiretapping. They further advised that we could not investigate wiretapping allegations other than to find out information about specific cases that we might have to dismiss or in which we would have to turn over information to defense attorneys. We advised Turner and Green to go see the FBI. I mean, they were bringing this to us, knowing we had no jurisdiction in the matter. We said, well, look, you go see the FBI. But we didn't stop there. We sent three people over to tell them about this information.

HODSON: So the important point, I think, for us is the fact that the FBI had information concerning alleged wiretapping in the Houston Police Department as early as about mid-1973.

VANCE: Yes. That's correct. And also Bob Bennett tells me that he had made Ron Waska, the Assistant U.S. District Attorney, aware of all of this.

HODSON: Ron Waska is?

VANCE: An Assistant U.S. Attorney. He is still working on the case, I believe. And this was in July or August of '73.

HERSHMAN: We had testimony concerning the demeanor of the FBI agents and the aggressiveness with which they handled the case. I was wondering if your assistants perhaps got an indication of what direction the FBI was going to go in or how interested they were to receive this information.

VANCE: Well, I didn't feel that they were really interested in the thing. And on the other hand, I didn't feel that they ignored it either. Later on, after Chief Lynn came to me and claimed that his phone was tapped, and he had this friend by the name of J. O. Patterson—I don't know if you have heard about Patterson or not. But Patterson was the private investigator that Lynn took into his confidence and made all these tapes and everything. But

Patterson came over to our office and Patterson had strange looking gadgets and puts things on the phone and claims there might be some bug on this phone and all that. Well, I certainly didn't accept his conclusions even though I don't know anything about electronic surveillance or technical aspects of it. But, my reaction was, don't accept what he says at all. So I called the FBI and they in turn contacted the phone company, and a team of phone company people and FBI agents spent considerable time at our office and out at our homes—mine, Bob Bennett's, and other key people in our office that had constant conversations about organized crime activities and investigations—and found absolutely nothing. Of course, you know if there had been something there it could have been taken off. But I'm convinced if there was something there, it was not discovered by Patterson because he had these gadgets . . .

HERSHMAN: Wasn't Patterson in fact the subject of a Grand Jury from your office?

VANCE: Well, Patterson was indicted yesterday in Harris County for illegal possession of either cocaine or morphine and it's . . .

HERSHMAN: And also two weeks ago I understand he was convicted . . .

VANCE: He was convicted in San Antonio of some blue box fraud against the telephone company—by the use of some kind of blue box that you make illegal long distance calls.

HODSON: Mr. Vance, can I ask you whether you know anything about the aggressiveness or the lack of aggressiveness of the FBI in wiretap cases in the Houston area? I ask you this question because we have testimony from Chief Lynn and also from the former U.S. Attorney in Houston who indicated very strongly to the Commission that the FBI was totally uninterested—let's put it that way—in investigating these alleged wiretap cases in the Houston Police Department, and that was in 1974—in the latter part of 1974. Have you any knowledge about that?

VANCE: No, I really couldn't express an opinion on that. I just have no reason to believe that they have not been diligent unless you could come to that opinion because of this Avila and Zavala matter. But, here again, Bob Turner and Bill Green, the two lawyers that represented these two people, were making all kinds of allegations about the Police Department and the narcotics people, and they were running over and having conversations with people in the press, and stories would suddenly appear about these matters in the newspapers. I don't know what their motive was. I do think they picked up some narcotics cases as a result of this, because they were representing people in narcotics cases—but these stories kept hitting the newspapers, and it just appeared to me that they were trying to try the case in the newspapers and embarrass the Police Department for some reason.

HODSON: Embarrass the Houston Police Department?

VANCE: Yes. The Houston Police Department. I understand their coming and telling us what they did, and we investigated and the indictments were obtained as a result of what they told us. That I mentioned before. But, the hard thing for me to understand is the fact that they came over to us and told us about this wiretapping—which is fine and good—we need to have information like that. But then, we told them, look, you know as well as we do—I mean, they are lawyers—there is no Texas wiretapping statute. It's a Federal violation. You've got to go see the FBI. They're the ones who investigate it. Go directly to the U.S. District Attorney's Office. And yet, they never did that.

HODSON: Did they do that for the purpose perhaps of trying to get reversals of other cases where they were defense attorneys?

VANCE: Oh, I definitely think so, because many, many motions were filed . . .

HODSON: On the basis of the allegations of Avila and Zavala?

VANCE: Yes. Right. Well, not so much on the basis of their specific allegations, but because of the fact that they made allegations that there were many wiretaps. Because of these allegations—in my opinion—many motions were filed where lots of people had been subpoenaed into court, and lawyers had gone on a fishing expedition with the hope that they might get their case thrown out as a result of illegal wiretapping. Or perhaps with the hope that we might dismiss it rather than go through all of that sort of litigation. And there were—as I say—there were only two cases that were actually dismissed, and we didn't really do this because of their allegations, but the cases had some other weaknesses to them. And we just came to the conclusion that it would be in the best interest of justice to dismiss the two cases. But this is two out of hundreds.

HODSON: Let me ask you this. You know about the allegations of wiretapping in mid-1973.

VANCE: Yes.

HODSON: And then Chief Lynn, who I believe took over as Chief in . . .

VANCE: January 1974.

HODSON: And then Chief Lynn, who took over as Chief in January 1974, came to you, and according to his testimony, said that he had had several discussions with you where he advised you that he believed that there was widespread wiretapping going on inside the Houston Police Department. So that would be the second indication that you would have, tending to verify, I suppose, Avila and Zavala's allegations. Did you take any further action at that time to advise him that he should go to the FBI or to advise him that he should go to the U.S. Attorney?

VANCE: Well, it was my understanding that the FBI was still investigating the matter. In fact, the matter is not completed to this day. He told me that he was going to go to the FBI and he was going to go to the U.S. District Attorney . . .

HODSON: And you told him that you couldn't prosecute for wiretapping in any event. Is that correct?

VANCE: That's right.

HERSHMAN: Why then did he come to you? Are you his legal advisor?

VANCE: We're not officially his legal advisor, but I mean any sheriff or any Chief of Police, if they have any confidence at all in the District Attorney, they're going to have a fairly close relationship and they're gonna seek advice from me. But he didn't come to me and say there's been a whole bunch of wiretapping. He knew what Avila and Zavala had been alleging all the time about these allegations. But he came to me and told me that he was doing an internal investigation into his own department and that I would be very surprised at some of his findings. And he did not discuss any specific cases with me then. And I told him that if it gets to the point that any of the officers have violated the State law and if you've got the evidence to support that, I want to hear from you, and I want to know about it, and I'll help you on it. I'll give you all the cooperation I can. But I said I don't want to go on some fishing expedition, and I said I don't want some third- or fourth-hand hearsay that I'm going to prosecute under. I said to him, you know with you it may be an administrative matter and you can fire some people or do whatever you do down there, but I'll get involved if we have some cases that have some evidence to them. We can look at the thing and if there are some officers doing wrong, we'll prosecute them.

HODSON: Let me . . .

VANCE: And it was just about that simple. But he did not come to me at that time with a whole bunch of things about wiretapping. He didn't really discuss specifics. He just said that he had an internal investigation going on, and that I was going to be surprised at some of the findings, and that he hoped to conclude this thing because the department is in turmoil over . . .

HODSON: I think we can button this up with just a couple of more questions, at least from me. One is, did he ask you specifically to make any investigation of the internal problems of the Houston Police Department?

VANCE: No, and of course, I wouldn't have any jurisdiction to do that.

HODSON: You would not have any jurisdiction?

VANCE: No. Not unless somebody made some allegation that someone had violated the law. And he told me . . .

HODSON: Well, I mean if he alleged the Houston Police were engaging in illegal wiretapping and then asked you if you would provide your investigative force to conduct the investigation, what would your reaction be?

VANCE: Well, I couldn't do that . . . to just look at wiretapping. But I would certainly make all the resources of my office available to try to look into the matter and interview the same people that he had interviewed to try to get to the bottom of the situation so we might dismiss other cases that might be affected. But this is why I wrote the letter. I was unaware—I knew that he was aware of these allegations of some wiretapping in the Narcotics Division, but when he came out and testified before the Congressional Committee, and before your Commission about literally thousands of wiretaps, or hundreds—on a grandiose scale that was so different from my general impression—this was the first I had ever heard it even expressed in those terms. And it was in a context so much different from that we had discussed previously, that I wrote this letter to him, because I wanted it in writing, and I wanted his reply in writing. I felt that he should have known enough law to know that anything defensive in nature has to be turned over to the defense attorney. I don't think I need to tell the Chief of Police that, but I certainly have reminded every Chief of Police in the jurisdiction of that fact since this occurred. I think they are all aware that anything defensive in nature must be disclosed—from all the seminars and information they get—they know that as well as they know that stealing is . . .

HODSON: What investigative capability do you have in your office? Have you ever, say in the last two or three years, reacted to a request from the Chief of Police to go down and use your own investigators to investigate an offense within the department?

VANCE: Oh, not some internal matter that would cause a person to be fired. I mean, if they came in and said so and so . . .

HODSON: Well, are your investigators employed in assisting the Assistant District Attorneys to prepare a case for trial or are they actually out on the streets looking into crimes at the basic stages?

VANCE: Our investigators are actually assisting the attorneys in preparing for trial. But we have approximately 11 lawyers who are in the Special Crimes Bureau with several investigators who do all types of original investigations so far as corruption goes—political corruption, fraud cases—somebody comes in with \$100,000 embezzlement from a bank. The police wouldn't touch it. They say go see . . .

HODSON: The Special Investigative Division.

VANCE: Yes. And we have indicted many people in public office—for public corruption—where we have done all of the investigations. We are very active.

HODSON: You do have a good investigative capability?

VANCE: Right. But they've got to bring me something to show that it is a Class A or B . . . a serious crime. There must be evidence of a serious misdemeanor or felony offense before I'm going to look into it; I'm certainly not just going to go on a fishing expedition on the basis of some hearsay.

HODSON: Do you have any knowledge that the Southwestern Bell Company might have had knowledge of these wiretaps?

VANCE: No. None at all. I know Jerry Slaughter, have known him a long time. He's been very cooperative in matters, and up until all of these things came out recently, I never heard anybody allege that Jerry Slaughter had ever assisted . . .

HODSON: I believe that concludes all my questions.

HERSHMAN: I just have one question. And this stems really from an interest in a similar wiretap case we had in New York

involving the Special Investigations Unit of the New York City Police Department. This was a case where widespread wiretapping was occurring by these police officers. My question is this: Is it conceivable—if in fact widespread wiretapping had occurred at the hands of the Houston Police Department, and evidence from that wiretapping was used in court cases—is it conceivable that the prosecuting attorneys would have no knowledge of that wiretap?

VANCE: It is certainly a possibility. I think it is highly unlikely. That's the only way I know to answer. It's a possibility, but it would be very remote, because I just don't think those officers keep that much to themselves.

HERSHMAN: —The New York . . .

VANCE: They are highly disciplined, but they don't keep that much to themselves.

HERSHMAN: In the New York case, it was brought out that the Assistant District Attorney did in fact have knowledge of it and possibly condoned it.

VANCE: Well—the thing is that you have that many people working with it in the Department, and somebody gets transferred, and he takes it bitterly—or even if he doesn't—he just gets transferred, or he's just having a few beers with his old buddy who is over on Radio Patrol, and he says, "Say, things are really different over here in Narcotics. Here's the way we do it." And I don't really—and even though I may be of the opinion that it was done in some cases at this point, I have no real proof. But I think there are very few cases—and by very few people out of a department of some 2,000 people. I think the whole thing is out of proportion a bit, the way some of the record stands now.

HODSON: You did indicate that after you got the allegation from Avila and Zavala that you did examine all the cases that you thought might be affected to see if you could find any evidence of wiretapping?

VANCE: Oh, yes. That's our instruction—to go over them case by case. This defendant. That defendant. Avila and Zavala would say, well this is on two people we don't know. When was it? So we'd go back in our files, and we came up with information pertaining to two cases.

HODSON: Mr. Vance, we appreciate your coming to Washington to let us interview you. Do you have anything else to add?

VANCE: No, I think we pretty well covered everything.

HODSON: This concludes the interview of Carol Vance, the District Attorney of Houston, by Michael Hershman and Kenneth Hodson. Thank you very much.

OFFICE OF THE

DISTRICT ATTORNEY

CAROL S. VANCE
District Attorney

SAM ROBERTSON
First Assistant

HARRIS COUNTY COURTHOUSE

HOUSTON, TEXAS 77002
713-228-8311

May 20, 1975

Honorable Carrol M. Lynn
Chief of Police
Houston Police Department
61 Riesner Street
Houston, Texas 77002

Dear Chief Lynn:

It has come to my attention from your testimony before the Texas Legislature that "thousands of illegal wiretaps" have been done by members of the Houston Police Department.

As you are aware, any evidence gained by means of illegal electronic surveillance would be inadmissible in evidence. Also, any conviction obtained, where such methods were utilized, could cause such conviction to be set aside. Further, under the Constitution of the United States, the State, by and through our office, has a positive duty to turn over any information that is defensive in nature to the defendant and/or his attorney. Such would include acts of illegal wiretapping. I can assure you that neither I nor any of my assistants know of any case presently pending nor any case in which a conviction has been obtained where illegal electronic surveillance methods have been used.

Since the duties of my office require that I disclose to the defendant any illegally obtained evidence and since our office, prior to prosecution, should review any cases in which illegal electronic surveillance was used, I therefore ask you and your department to provide me with a list of all persons or cases upon which any illegal electronic surveillance has been conducted. Further, I need the findings, the investigative reports, and any information under your control which would shed any light upon whether any illegal electronic surveillance was carried out in any case both disposed of or pending. This matter is of utmost urgency to our judicial processes.

I must have these findings and reports immediately as there are many felony cases from your department proceeding to trial each and every day. In my opinion this would not violate any "gag rule" of any Judge's pending case or investigation. I do not intend to make any of these matters public. I do intend to inform the appropriate trial judges and the attorney for the accused of any information that might be considered "defensive" in nature to his case.

Sincerely,

[Signed] CAROL S. VANCE
District Attorney,
Harris County, Texas

CSV:cw

cc: Honorable Edward McDonough, United States Attorney

Judge Garth Bates, 174th District Court
Judge William Hatten, 176th District Court
Judge Miron Love, 177th District Court
Judge Dan Walton, 178th District Court
Judge I. D. McMaster, 179th District Court
Judge Fred Hoey, 180th District Court
Judge Lee Duggan, Jr., 182nd District Court
Judge Joseph Guarino, 183rd District Court
Judge Wallace C. Moore, 184th District Court
Judge George Walker, 185th District Court
Judge Andrew Jefferson, Jr., 208th District Court
Judge Frank Price, 209th District Court

CITY OF HOUSTON

FRED HOFHEINZ, MAYOR
POLICE DEPARTMENT

C. M. LYNN, CHIEF OF POLICE
61 RIESNER STREET
HOUSTON, TEXAS 77002

TELEPHONE (713)222-3011, RADIO KKD 490,
TELETYPE 1 713 571 1012

May 30, 1975

Honorable Carol S. Vance
District Attorney
Harris County Courthouse
301 San Jacinto
Houston, Texas 77002

Dear Mr. Vance:

I have received your letter of May 20, 1975, which concerns any pending cases as well as any convictions which may have been obtained by your office where illegal electronic surveillance may have been utilized by this department. I understand the gravity of this situation and share your concern.

First, let me assure you unequivocally that since I became Chief of Police on January 9, 1974, no illegal electronic surveillance has been condoned or tolerated at any level of command in this department. I can, therefore, state that no case originating after January 9, 1974, is in any way tainted by any illegal means of investigation by this department. I realize, however, that this does not fully alleviate the problem.

When I became Chief of Police I was confronted with the indictment by a Federal Grand Jury of several officers of the Houston Police Department for alleged activities occurring prior to my appointment. This led to my investigation which resulted in the conclusion that illegal wiretapping had been utilized by some members of this department. I would like to emphasize that my only knowledge of this situation came as a result of the investigation and therefore is a conclusion, although a well supported one, on my part. I had and have no personal contemporary knowledge of any occurrence of illegal electronic surveillance. I, like you, know of no case presently pending nor any case in which a conviction was obtained where illegal electronic surveillance methods were used by this department.

In this connection, I would like to point out that in my testimony before the Texas Legislative Committee I stated, in response to persistent inquiry soliciting my opinion, that my conclusion based upon my investigation indicated that there may have been as many as 1000 illegal wiretaps. As stated to the Committee, this was and remains only my opinion.

While I am convinced that a substantial number of illegal wiretaps have occurred, I have no tangible evidence that any of them ever resulted in any criminal charge, indictment or conviction, although in candor I must concede that I believe the probabilities are otherwise.

As you can well realize, if from nothing else than the number of officers or former officers who have invoked the privilege against self-incrimination before legally constituted investigating bodies where testimony is obtained under oath, my investigation was a very difficult one and resulted in the discovery of relatively few specific cases where illegal wiretapping may have been utilized. Any such specific cases would be identified on the tape cassettes now in the possession of the Federal Grand Jury. I do not have a copy of either these tapes or the transcripts made from them. Nor, after this period of time, do I have any independent recollection of any specific cases that may be disclosed from these sources. I assume that the tapes in possession of the Grand Jury are possibly more available to you than they are to this department, however, if it would be a convenience to you, and the Grand Jury will permit, I will detail personnel of the Houston Police Department to review such tapes and make excerpts for your use of any specific cases identified in them.

My investigation did disclose that at one time there may have been maintained in the Houston Police Department a log of the persons who were issued electronic surveillance equipment that apparently was available within the department. This log, as well as all such electronic surveillance equipment, had disappeared prior to my appointment as Chief of Police and my investigation indicates that it was destroyed. My investigation indicates that no list of cases in which any illegal electronic surveillance was conducted was ever kept, and it appears to me improbable that any such list ever existed. Notwithstanding the fact that I stated on a television interview that such a list might be prepared with two years of intensive investigation, in retrospect and after considering the obstacles to such an investigation, I feel that no meaningful list of such activities could ever be prepared.

The only thing that I can suggest at this time that may assist in solution of the current problem is for your office, in preparing

any case for trial, to interrogate the investigating officers as to whether any illegal electronic surveillance was conducted in the investigation and if you are not satisfied with the result of such interrogation, advise me and I will make as thorough an investigation of the investigation methods used in such case as is possible. As to those cases in which your office obtained convictions based upon investigations by this department prior to January 9, 1974, I hope that the investigation of the U.S. Attorney's Office and the Federal Grand Jury will provide, or at least point to, a solution. As you probably know, following the conclusion of my basic investigation, I, upon the advice of my attorney, turned over to the United States Attorney and the Federal Grand Jury all of my investigative reports and they have been conducting a continuous investigation of this matter since that time. In the event, however, that their investigations do not adequately solve this problem, I will consider any recommendation that you or the City Attorney may have as to review of such convictions by this department.

I both understand and regret the burden that this is placing upon your office. I hope you understand that this has been a painful and disruptive situation in the Houston Police Department. I can only say that the disclosure and investigation of this situation was necessary and will certainly enable your office and the Houston Police Department to better achieve our mutual goal of proper law enforcement.

Sincerely,

[Signed] C.M. Lynn
Chief of Police

CML:eps

cc: Honorable Edward McDonough, United States Attorney

Judge Garth Bates, 174th District Court
Judge William Hatten, 176th District Court
Judge Miron Love, 177th District Court
Judge Dan Walton, 178th District Court
Judge I.D. McMaster, 179th District Court
Judge Fred Hooey, 180th District Court
Judge Lee Duggan, Jr., 182nd District Court
Judge Joseph Guarino, 183rd District Court
Judge Wallace C. Moore, 184th District Court
Judge George Walker, 185th District Court
Judge Andrew Jefferson, Jr., 208th District Court
Judge Frank Price, 209th District Court

CHAIRMAN ERICKSON: We will take a five-minute recess.

[Whereupon, a short recess was taken.]

CHAIRMAN ERICKSON: If we may reconvene, Jerry Bragan, will you come forward, please?

[Whereupon, Jerris E. Bragan was sworn by Chairman Erickson.]

TESTIMONY OF JERRIS E. BRAGAN, CONVICTED PRIVATE INVESTIGATOR

CHAIRMAN ERICKSON: Our next witness is Jerry Bragan, former private investigator in the Washington area who was convicted in May 1973 of Title III violations committed in the course of several of his investigations. Mr. Bragan will discuss the attitudes of the private investigator toward the provisions of the Federal Wiretap Act.

MR. HERSHMAN: Mr. Bragan, what is your current occupation?

MR. BRAGAN: I am working for a retail chain in security.

MR. HERSHMAN: In private security work?

MR. BRAGAN: Yes.

MR. HERSHMAN: May I ask: Did you hold a private investigator's license in the Virginia area?

MR. BRAGAN: Yes, I did.

MR. HERSHMAN: When was that?

MR. BRAGAN: The exact dates I don't recall. It was '72 and '73.

MR. HERSHMAN: When did you first get into the private investigative business?

MR. BRAGAN: In 1969.

MR. HERSHMAN: Would you give us a brief description of how you started in it and what your positions were?

MR. BRAGAN: Well, I started part-time working for Wackenhut Corporation here in Washington, went from there to Searches as General Manager, and then set up my own company.

MR. HERSHMAN: And when you were involved with these other companies, Wackenhut and Searches, were you involved in private investigative work?

MR. BRAGAN: Yes.

MR. HERSHMAN: What type of cases did you handle?

MR. BRAGAN: With Wackenhut it was principally work for insurance companies suspected of fraud of one sort or another—some chasing of wandering spouses as all agencies handle: missing persons. I didn't get into any criminal work with Wackenhut at all. At Searches, mostly domestic work, missing persons—this type of thing.

MR. HERSHMAN: Did you have occasion to use electronic surveillance while working for these two organizations?

MR. BRAGAN: I personally didn't, no.

MR. HERSHMAN: Do you know of its use by others within these organizations?

MR. BRAGAN: Yes.

MR. HERSHMAN: Was its use legal by these other individuals?

MR. BRAGAN: Well, if there had been any questions of it at the time, I probably wouldn't be sitting here now. I don't recall the question ever being raised as to its legality at all. They were all situations that involved the parties or the clients' own phones and premises—never any question about it.

MR. HERSHMAN: So up to the time when you formed your own agency you had no real exposure to electronic surveillance in one form or another?

MR. BRAGAN: Except for seeing some of the equipment, a couple of transmitters and telephone switches, and this sort of thing, no.

MR. HERSHMAN: Well, did you consider at that point that you were technically capable of performing a wiretap?

MR. BRAGAN: Oh, good heavens, no. I am still not, for that matter.

MR. HERSHMAN: Tell me, Mr. Bragan, how did it first come about that you engaged in illegal wiretapping or bugging?

MR. BRAGAN: For my company are you referring to now?

MR. HERSHMAN: That is right. I assume this was in 1972; is that right?

MR. BRAGAN: Yes. Very briefly, we were retained by an attorney in Washington to handle a domestic case for him. And as a matter of fact, he had had Wackenhut working on the case prior to that time. And he wanted to have a telephone tap installed on this particular individual's telephone.

We discussed the various aspects of the law as he explained it to us, and finally agreed that the type of tap he wanted put on, on a doctor's phone—there had been all kinds of problems getting involved in privileged communications between a doctor and patient and so on, so ultimately he requested what we get was a room bug which was obtained from a firm in Baltimore. And the client, that is, the wife, installed it in her husband's bedroom herself, and we monitored the transmissions.

The only thing that was being overheard was her husband's conversations with his mistress on the telephone.

MR. HERSHMAN: Did this attorney tell you that this would be an illegal act?

MR. BRAGAN: No; no. As he explained it to us at the time, as long as it was on the client's—whoever that was—their own property and their own phones and this type of thing, there wouldn't be any problem. The only reason there was a problem in putting a tap on this particular telephone was because, as I said, the communication between the doctor and some of his patients and that sort of thing, and he felt that would be getting into a questionable area, so we didn't get a tap on that.

MR. HERSHMAN: This being the first time you did it, how did you go about it?

MR. BRAGAN: I don't honestly recall how I got in touch with this fellow in Baltimore. One of your investigators asked me the same question, and this goes back three or three-and-a-half years ago, and I just don't recall how I got his name.

I have a vague recollection of talking to a Prince Georges County fellow about him, but I can't honestly recall how I got in touch with him.

MR. HERSHMAN: Obviously, you had to buy the equipment from someone?

MR. BRAGAN: Yes.

MR. HERSHMAN: And he had to teach you or show you how to use it; correct?

MR. BRAGAN: It was a relatively unsophisticated device. It was simply putting the hearing aid battery into it and he sold us the transmitter and a modified FM radio receiver.

MR. HERSHMAN: You keep saying "us." Did you have an employee or partner?

MR. BRAGAN: I had a partner, yes.

MR. HERSHMAN: What was his name?

MR. BRAGAN: Jerry Cavanaugh.

MR. HERSHMAN: You say you gave this device to the woman to plant in her husband's room?

MR. BRAGAN: She was living in the house at the time. We went into the house with her and looked over the layout, and we experimented with various places of putting it and monitoring it. She ultimately changed it around to some other place. That was the only time we went into the house.

MR. HERSHMAN: Where was the receiver for the device?

MR. BRAGAN: Well, it was a portable receiver that we had in a car.

MR. HERSHMAN: And did you make tape recordings of his conversations?

MR. BRAGAN: Yes.

MR. HERSHMAN: What did you do with the tape recordings?

MR. BRAGAN: They were turned over to the attorney.

MR. HERSHMAN: Do you know what the attorney did with these?

MR. BRAGAN: To put them in the vernacular, I think he gathered the intelligence from them to sandbag the doctor's secretary or nurse, or whatever she was. I found out later they implied that through some kind of reverse set-up with their house intercom, they had overheard conversations. I don't know if they testified to that or implied that or what.

MR. HERSHMAN: Did the woman get a divorce eventually?

MR. BRAGAN: Yes, she did.

MR. HERSHMAN: Do you know if any information obtained from this bug was used in the court trial?

MR. BRAGAN: Not directly, no.

MR. HERSHMAN: Was the husband ever aware that he was the victim of a bug?

MR. BRAGAN: I doubt it very seriously—even to this day.

MR. HERSHMAN: How much were you paid for that job?

MR. BRAGAN: It would be a combination of some very long-term surveillance. I charged her for the equipment exactly what we paid for it, which was \$250 for the transmitter and receiver. The total case involved \$1200 or \$1300, something of that sort.

MR. HERSHMAN: So here it was, your first year in business. You had really minimal experience in the private investigative field. You went to an attorney and he suggested that a listening device be placed in this man's room; is that correct?

MR. BRAGAN: That is correct.

MR. HERSHMAN: And this was your entrance into the field of illegal electronic surveillance?

MR. BRAGAN: Rather ironically, one of the reasons our whole business was related to attorneys—we didn't take any clients or any cases. We had an ad in the yellow pages, but we didn't take any cases where a person wasn't represented by counsel to avoid exactly this kind of problem—not just wiretap but trouble with the law. The answer to your question is yes.

MR. HERSHMAN: When was the next occasion that you used illegal electronic surveillance?

MR. BRAGAN: The next occasion, I guess, would be the two cases that I was subsequently indicted and convicted on.

MR. HERSHMAN: Can you give us the circumstances of those cases?

MR. BRAGAN: Very briefly, one of them was a big case where our client, a relatively prominent local contractor, had been embezzled out of some \$200,000 or \$300,000. The other case involved a government employee who was seeking a divorce from his wife, who was calling various high officials in the government and accusing them of all kinds of—

MR. HERSHMAN: At this point did you still have your original partner, Mr. Cavanaugh?

MR. BRAGAN: I had a new partner at this time.

MR. HERSHMAN: Who was that?

MR. BRAGAN: A fellow I knew at that time as William R. Raymond.

MR. HERSHMAN: And did you subsequently find out that Mr. Raymond was not Mr. Raymond after all?

MR. BRAGAN: Oh, yes.

MR. HERSHMAN: Who was Mr. Raymond?

MR. BRAGAN: Patrolman William R. Phillips of the New York City Police Department.

MR. HERSHMAN: And who was Patrolman Phillips?

MR. BRAGAN: He was a fellow that was nailed by the Knapp Commission in the process of putting

Xaviera Hollander on the pad. In exchange for immunity he went to work undercover for the Knapp Commission, and was subsequently indicted for two counts of murder and one count of attempted murder.

MR. HERSHMAN: He was a corrupt New York City police officer?

MR. BRAGAN: Very definitely.

MR. HERSHMAN: And what was Mr. Phillips doing down here under the name of Mr. Raymond?

MR. BRAGAN: Well, I found out later he was under what you would call the federal witness program. There had been numerous threats against his life. His name had been changed. Up until, I believe, about a month before he became associated with me, he was under the protection of U. S. Marshals. In fact, after that, whenever he went back to New York, he had a bevy of marshals with him protecting him.

MR. HERSHMAN: You mean the federal authorities gave him a change of identity and protected him?

MR. BRAGAN: Plus paying him a per diem while he was down here.

MR. HERSHMAN: Did Mr. Phillips have to get a license in order to practice private investigation in Virginia?

MR. BRAGAN: Yes, he did.

MR. HERSHMAN: What procedures did you go through to get his license?

MR. BRAGAN: The procedures in Alexandria are supposed to be efficient. You are fingerprinted by the police department and the prints are sent through the FBI for clearance, and when they come back you are issued a license.

MR. HERSHMAN: Was Mr. Phillips given clearance?

MR. BRAGAN: Yes, he was.

MR. HERSHMAN: In other words, you had no idea that the man you were hiring as your partner was, indeed, not only a corrupt New York City police officer but was under indictment for murder at the time in New York?

MR. BRAGAN: That is correct.

MR. HERSHMAN: Has he since been convicted of murder?

MR. BRAGAN: Last fall he was convicted on both counts of murder and attempted murder and is serving two life sentences in Attica right now.

MR. HERSHMAN: What role did Mr. Phillips play in aiding you on these illegal wiretaps down here?

MR. BRAGAN: Originally he came into the company as a partner. There was three of us, Mr. Cavanaugh and Raymond and myself. Phillips is an exceptional investigator, and after a very short

period of time both Cavanaugh and I thought it would be much more to our interest to have him as a partner in the company rather than going out and setting up his own, which he did.

He was with me when we interviewed both of the clients that I referred to.

Backtracking just a bit, in June, which would have been about two or three months before I met Phillips, a fellow named Lindsey had run an ad in the *Washington Post* for transmitters—this was right around the time of the first case I was talking to you about—and he came over with a suitcase full of various goodies, none of which I had the time or money or interest in at the time. Phillips was very interested in this.

MR. HERSHMAN: Let me just interrupt now. He ran an ad for what in the *Washington Post*?

MR. BRAGAN: I have forgotten exactly. It was under the title, "Items for Sale"—transmitters—a two- or three-line ad about wireless transmitters for sale.

MR. HERSHMAN: And he brought over, after you called him, a suitcase full of equipment?

MR. BRAGAN: Yes, various types of equipment.

Phillips was interested in meeting Lindsey. The only thing we knew about Phillips at the time was he had allegedly been an undercover agent for the Federal Government investigating organized crime in New York—this sort of thing. When he was cleared in Alexandria, there was no further problem.

At any rate, he talked about some of the wire-tapping he was familiar with in the government, was very interested in the subject, said he'd know whether some of this equipment Lindsey had was worthwhile or not.

So I called Lindsey and he came over and brought basically the same equipment over again.

This was, oh, perhaps a month or six weeks before this industrial case came into the office that I referred to.

MR. HERSHMAN: Did Mr. Phillips feel that the way to make money in this business was through wiretapping and bugging?

MR. BRAGAN: His basic premise was that in terms of gathering information, intelligence on various cases, it would be very worthwhile.

MR. HERSHMAN: How about you? How did you feel about it?

MR. BRAGAN: Under the restrictions as I understood them, certainly; it is very beneficial.

MR. HERSHMAN: What restrictions are you speaking of?

MR. BRAGAN: That is, you know, you come to me and ask me to bug Professor Blakey's telephone; as I understood it at the time, that would be clearly illegal. No, not that sort of thing.

MR. HERSHMAN: When you applied for your license as a private investigator, did they give you a copy of the Title III regulations?

MR. BRAGAN: No.

MR. HERSHMAN: Did anyone talk to you about what is legal or illegal about electronic surveillance?

MR. BRAGAN: The only person I discussed this type of thing with at all was the attorney I mentioned to you earlier.

MR. HERSHMAN: So no official of the state talked to you as a prospective private investigator about the pitfalls of using electronic surveillance?

MR. BRAGAN: To the best of my knowledge, there is no jurisdiction in the U. S. that does so.

MR. HERSHMAN: If you had had knowledge of the provisions of Title III and understood them, do you feel perhaps you wouldn't have engaged in this activity?

MR. BRAGAN: I was running a very successful and profitable business. We didn't need illegal wire-tapping.

CHAIRMAN ERICKSON: I think it is safe to say this attorney who gave you the advice on Title III was probably not very well-informed.

MR. BRAGAN: I don't think it was malicious, no.

MR. BLAKEY: It sounds to me like you've got a malpractice suit.

MR. HERSHMAN: Let's go on.

I believe you had meetings with other attorneys. You talked about this government official. Obviously, an attorney was involved in that case, too, where you wiretapped his wife; is that correct?

MR. BRAGAN: What are you referring to now?

MR. HERSHMAN: I am referring to the Davenport case.

MR. BRAGAN: Oh, yes.

MR. HERSHMAN: Did you talk to his attorney about the possibility of using this device?

MR. BRAGAN: No, that was not discussed. This is one of the things the U. S. Attorney was very excited about, that there would be a lot of lawyers involved.

MR. HERSHMAN: So we have these two cases coming up, the marital case and the business case. Would you tell us where you got the equipment and how that was accomplished?

MR. BRAGAN: From Mr. Lindsey.

MR. HERSHMAN: Did you hire Mr. Lindsey?

MR. BRAGAN: Ultimately he came to work for the company full time.

MR. HERSHMAN: What was Mr. Lindsey's background?

MR. BRAGAN: Electronics.

MR. HERSHMAN: Was he a radio and TV repairman?

MR. BRAGAN: Yes.

MR. HERSHMAN: And you hired him to help you investigatively?

MR. BRAGAN: Not just in the area of electronics.

MR. HERSHMAN: Did he have any investigative experience?

MR. BRAGAN: Oh, no.

MR. HERSHMAN: Then I think it's safe to say his expertise would fall in the area of electronic matters.

MR. BRAGAN: He wasn't happy about it, but in the Furman case we put him out on a construction job with a broom.

MR. HERSHMAN: What was used in the Furman case?

MR. BRAGAN: Three telephone taps, basically. They are about the size of a 50-cent piece and about a quarter-of-an-inch thick, attached to the telephone lines. They had a broadcasting range of about a half-mile. The transmitters didn't activate until the telephone receiver was actually picked up, created no interference or anything of this sort on the line.

In a car that Phillips rented, the receivers had been installed so that the vehicle could be left unattended and still the conversations monitored at a later date.

MR. HERSHMAN: Who installed the equipment?

MR. BRAGAN: Lindsey.

MR. HERSHMAN: Who monitored the conversations?

MR. BRAGAN: Lindsey and a fellow by the name of Flurry and a fellow by the name of Steve Zorn. Phillips was out there on one or two occasions.

MR. HERSHMAN: And the listening post was in a car Mr. Phillips had rented?

MR. BRAGAN: Right.

MR. HERSHMAN: Why were these phones being monitored?

MR. BRAGAN: The client, Mr. Furman, had reason to believe that three of his employees had embezzled several hundred thousand dollars from his company when he was in the process of converting from a handwritten method of bookkeeping over to a computerized system. It was believed that they were involved with several other conspirators. And his company at that time was in a virtual state of collapse. He was getting no cooperation out of the Montgomery County officials he went to to get an investigation going. They since have indicted these people, I understand, or were going to—I don't know.

And it was everybody's general opinion that putting taps on these telephones would expedite the investigation in the quickest possible manner, basically to find out who else they were dealing with outside of the company—suppliers and a few other people.

MR. HERSHMAN: Who suggested that wiretaps be used in this case?

MR. BRAGAN: Oh, I think the original suggestion came from Phillips. This is an area where he was supposedly an expert.

MR. HERSHMAN: And it was thoroughly discussed with Mr. Furman, the owner?

MR. BRAGAN: Oh, yes.

MR. HERSHMAN: Now, what did you charge Mr. Furman for this investigation?

MR. BRAGAN: I think our cost on the equipment was \$1100, which we charged him—and we charged him the same thing we paid for the equipment. I think the total fee came to about \$10,000.

MR. HERSHMAN: And how was the information used that was obtained from the wiretaps?

MR. BRAGAN: Pardon?

MR. HERSHMAN: How was the information used that was obtained from the wiretaps?

MR. BRAGAN: It wasn't. Before the case was concluded the Justice Department had just about everything.

MR. HERSHMAN: You mentioned that at the same time you then began your second domestic wiretap case. Can you tell us how you got into that?

MR. BRAGAN: That was the Davenport case. I don't know whether Furman came first or Davenport, but both of them were within a couple days of each other.

It was just basically a standard type domestic case. The only complication involved was that he was high-placed in the government, and his wife was calling various people and creating a lot of problems for him, or he believed she was. It is the same type of tap I described earlier. It was installed on the telephone wire.

MR. HERSHMAN: By whom?

MR. BRAGAN: Lindsey.

MR. HERSHMAN: Was Mr. Phillips also involved in this tap?

MR. BRAGAN: Oh, yes.

MR. HERSHMAN: Where did it transmit to?

MR. BRAGAN: It didn't transmit at all. It was a faulty transmitter.

MR. HERSHMAN: Wasn't this the tap that was originally discovered by the police?

MR. BRAGAN: Yes, it was.

MR. HERSHMAN: How did that come about?

MR. BRAGAN: Well, I didn't see the installation. I never did see the thing. But according to Mc-

Donald and the Arlington County detectives I talked to about it later, it was a pretty sloppy job. The wiring itself was apparently covered with gray tape and Lindsey just spliced the lines and covered it with black tape and left alligator clips and other choice things lying on the ground. Mrs. Davenport discovered it and thought something was peculiar and called Arlington and they in turn called the FBI.

MR. HERSHMAN: Can you tell us how the case proceeded from there?

MR. BRAGAN: Just generally, the complicated interplay of personalities there—about the same time I decided to terminate Phillips' relationship with the company.

MR. HERSHMAN: Why was that?

MR. BRAGAN: I was pretty well satisfied—I had found out by this time who he was and I was pretty well satisfied that his complaints of a police frame didn't sound quite as good as they originally did when he proffered them.

MR. HERSHMAN: When you terminated him, was it then Mr. Phillips started working as a government agent against you?

MR. BRAGAN: Yes. He said if he was terminated that he'd go to the FBI; that he was a federal witness and the government would protect him, and he would send everybody down the tube, et cetera, et cetera.

MR. HERSHMAN: Was Mr. Phillips eventually granted immunity in this case?

MR. BRAGAN: Yes, he was.

MR. HERSHMAN: So here we have an indicted corrupt New York City police officer who engaged in wiretapping down here, and he was granted immunity in order to testify against you; is that correct?

MR. BRAGAN: That is right.

MR. HERSHMAN: Was anyone else granted immunity in order to testify against you?

MR. BRAGAN: Mr. Furman was. Professor Butler was. Lindsey was. Everybody was.

MR. HERSHMAN: Was anyone else convicted on these charges aside from you?

MR. BRAGAN: Nobody else was even charged.

MR. HERSHMAN: And you were a full partner with Mr. Phillips in this corporation, is that not the case?

MR. BRAGAN: That is correct.

MR. HERSHMAN: How long was this corporation set up?

MR. BRAGAN: How long had it been in business?

MR. HERSHMAN: Yes.

MR. BRAGAN: It had been in business, I believe, a little over a year at that time.

MR. HERSHMAN: Can you tell me during this year's period how many times you were approached to do illegal wiretap or bugging jobs?

MR. BRAGAN: Oh, the exact count I couldn't tell you. I would guess that by recollection—we might get a couple of calls a week.

MR. HERSHMAN: Would you say maybe 50 or 60 times during that year?

MR. BRAGAN: Yes.

MR. HERSHMAN: So the business is out there if you really want it, isn't it?

MR. BRAGAN: Oh, good heavens, yes.

MR. HERSHMAN: Is it generally the case that more money is charged when you use wiretapping?

MR. BRAGAN: Well, I don't know that anybody else does. That is generally the impression you get in the profession, what you hear various places from people. It is a question of supply and demand.

MR. HERSHMAN: What about the profession? Were you aware of other private investigators in the country doing the same thing as you?

MR. BRAGAN: Well, you hear things. I knew of more police officers that were involved in illegal tapping than private investigators. But as far as direct personal knowledge, no.

MR. HERSHMAN: Did you perhaps gain a reputation whereby people would be referred to you because you handled this type of activity?

MR. BRAGAN: I wouldn't think so because basically it was just those cases involved. There wasn't anything discussed as any particular big deal, you know, with anybody one way or the other.

MR. HERSHMAN: What determined whether you'd take a case involving illegal wiretap?

MR. BRAGAN: Well, basically whether the necessity for this type of activity warranted the expense; whether, you know, it involved the client's own telephones and premises or not.

MR. HERSHMAN: And the equipment to do this was readily available; is that correct?

MR. BRAGAN: Oh, yes. I would have to disagree with one of your manufacturers. Even though I am not a technician, Lindsey is certainly not one of the budding electronic geniuses of the day, and he certainly made some very fine equipment. I know a few people that are involved in radio and TV repair that tell me if they have the schematics and the equipment that they can build just about anything; it is no problem.

These basement shops that one of the fellows talked about earlier this morning, I think, is probably where most of the illegal equipment comes from.

MR. HERSHMAN: Mr. Bragan, do you have any recommendations as to possible licensing procedures for private investigators that would toughen the system up?

MR. BRAGAN: Well, I think the licensing regulations from state to state and jurisdiction to jurisdiction are just—they are a mishmash of virtually nothing except maybe a handful. Certainly there should be some requirement where private investigators have a better understanding of the wiretap law.

Because I will tell you right now there is no doubt in my mind that there are a lot of private investigators involved in wiretapping of one sort or another that probably are not aware of some of the serious criminal penalties involved, the illegality of it.

MR. HERSHMAN: Mr. Bragan, how many counts of illegal wiretapping were you convicted of?

MR. BRAGAN: They took two cases and stacked them up to six counts.

MR. HERSHMAN: And what was your sentence?

MR. BRAGAN: Two years, 18 months suspended, six months confined to Allenwood.

MR. HERSHMAN: Thank you.

CHAIRMAN ERICKSON: Chief Andersen.

MR. ANDERSEN: I have no questions.

CHAIRMAN ERICKSON: Judge Shientag.

MS. SHIENTAG: No questions.

CHAIRMAN ERICKSON: Professor Blakey.

MR. BLAKEY: You mentioned you knew more police than private detectives who did surveillance. What area is this?

MR. BRAGAN: In the Washington metropolitan area.

MR. BLAKEY: D. C. police?

MR. BRAGAN: Yes, sir.

MR. BLAKEY: Arlington police?

MR. BRAGAN: No.

MR. BLAKEY: Prince Georges County police?

MR. BRAGAN: Yes, sir.

MR. BLAKEY: Have you ever been interviewed by the Bureau?

MR. BRAGAN: Sir?

MR. BLAKEY: Have you ever been interviewed by the FBI in connection with your knowledge of illegal police surveillance?

MR. BRAGAN: No.

MR. BLAKEY: Have you ever indicated to them that you had it?

MR. BRAGAN: No.

MR. BLAKEY: Have you ever indicated to any other law enforcement agency that you had it?

MR. BRAGAN: Other than to the investigators of this Commission, I don't believe I have discussed it with anybody; no.

MR. BLAKEY: How old is the information?

MR. BRAGAN: Well, one of them would go back about two years. The other, out in Virginia, I would imagine is still going on.

MR. BLAKEY: Needless to say, Mr. Chairman, I suggest the transcript of this part of this witness' testimony be made available to the Department of Justice for such action as it sees fit.

Thank you.

CHAIRMAN ERICKSON: I might ask this: In connection with your conviction for violation of Title III, presentence investigation report was made, was it not?

MR. BRAGAN: I believe so, yes.

CHAIRMAN ERICKSON: And you are on probation at the present time?

MR. BRAGAN: That is right.

CHAIRMAN ERICKSON: In talking to the probation officer, you certainly told him how widespread this was, didn't you?

MR. BRAGAN: I think I may have spoken with Mr. Sullivan a total of two minutes.

CHAIRMAN ERICKSON: In other words, that is all your probation interview consisted of?

MR. BRAGAN: My probation interview really wasn't much of an interview. I think he asked me my address and asked me to give him something in writing. That was the extent of it.

CHAIRMAN ERICKSON: Your statement wasn't, "Why me? It's going on everywhere else," was it?

MR. BRAGAN: No, it was not.

CHAIRMAN ERICKSON: You didn't state that to the U. S. Attorney or anyone in connection with it? Did you tell your own lawyer it was kind of unusual you had been singled out?

MR. BRAGAN: My lawyer was Philip Hirschkop. He thought it was rather unusual, too.

CHAIRMAN ERICKSON: You didn't think that was unusual, that everybody else walked by without getting indicted and suddenly here you are, the proud possessor of a felony indictment?

MR. BRAGAN: Mr. Chairman, for a period of about three months I was in a state of shock. I didn't do too much wondering about anything, frankly.

CHAIRMAN ERICKSON: When you were talking to your lawyer, didn't you tell your lawyer, "This is the reason I did it. I was given this bad advice by another lawyer and I acted on the basis of that, and everybody else is doing it so I couldn't see that it was too bad."

MR. BRAGAN: The federal judge refused to admit that as evidence.

CHAIRMAN ERICKSON: You mean it was offered? You testified to that?

MR. BRAGAN: Yes.

CHAIRMAN ERICKSON: Was an offer of proof made?

MR. BRAGAN: Yes.

CHAIRMAN ERICKSON: So at the time this was before the court it was made clear that there were other violations that were known to you?

MR. BRAGAN: Yes.

CHAIRMAN ERICKSON: Well, Mr. Bragan, we are deeply indebted to you for taking your time to give us your experience with Title III. It does have some teeth though, doesn't it?

MR. BRAGAN: It certainly does.

CHAIRMAN ERICKSON: Thank you very much for appearing.

[The relevant material follows.]

AVAILABILITY OF ELECTRONIC SURVEILLANCE SERVICES TO THE GENERAL PUBLIC

In April of 1975, the National Wiretap Commission staff initiated a survey of private investigative agencies in six cities in the United States. The purpose of the survey was to determine the types of electronic surveillance services and countermeasures that were available to the general public. The staff did not intend to identify the private investigators who offer such services, but wanted only to determine the extent to which the public has access to debugging and wiretapping expertise. The staff was also interested in the number of investigators who would be willing to broach the subject of conducting offensive electronic surveillance in the course of a telephone conversation. Although most were hesitant to discuss the matter in detail by telephone and requested private meetings, a substantial number volunteered specific suggestions on methods, devices, and costs of offensive surveillance measures. Finally the survey attempted to discover what information the investigators provided as to the legality of such services.

In seeking this information, the Commission staff randomly chose seven cities in which to conduct the survey. A member of the staff attempted to contact private investigative agencies listed in the yellow pages of each city's telephone directory. In those instances where two or more agencies listed the same telephone number, or where the listing indicated that one agency was associated with another, only one of the related agencies was contacted. The response from that agency was assumed to be the same for all agencies associated with it.

The Commission staff member would call an agency and ask to speak with an investigator. The investigator was told that the caller was a local businessman with a suite of twelve offices. He was told that the caller's firm had been experiencing a loss of business and that the caller suspected two possible causes: first, that confidential conversations and strategies were being overheard by a competitor; second, that one or possibly two of the firm's consultants were engaging in outside business activities of which the caller was not aware. The caller then asked for a cost estimate of having the offices checked for listening devices, and for information on the feasibility and legality of overhearing the office and telephone conversations of the two consultants.

The results of the survey reveal that of 115 firms contacted in seven cities, 71 provide debugging services and 42 either offered to perform offensive wiretapping and bugging themselves or referred the caller to another specified agency that would provide this service. The estimated costs of the debugging operation varied widely, and many agencies insisted on seeing the offices before giving any estimates. The estimates given over the phone ranged from \$80 to \$3,480. The costs of setting up means by which the businessman could overhear his consultants' conversations were estimated as low as \$30 and as high as \$5,000, and suggested methods ranged from simple tape recorders to a closed circuit TV.

In Atlanta, of 28 firms contacted, 18 indicated they would provide debugging services, and 14 also offered to perform offensive wiretapping and bugging. One investigator suggested that the possibility of monitoring a consultant's conversation "would be very good, no problem at all." One hinted that they would be on a "little shaky ground," but suggested using a tape recorder or microphone transmitter in the false ceiling of the consultant's office. He explained that a telephone monitoring system could be set up by attaching an induction coil, bought at the Radio Shack, to the phone. Whenever the consultant made a call, the businessman could remove his receiver and record the conversation. Another, referring to setting up a phone monitoring system, said that there were several ways in which this could be accomplished. He specifically stated that he could set up the telephone so that the businessman could monitor calls or "we have a system where we can hook it up and listen over a transistor radio." One agent stated that although his firm did not do offensive surveillance, he "might be able to make the connections with the right people who can get you the equipment." Another investigator stated that he possessed the equipment needed to do the overhearing and that he would do it. One investigator explained that although he did not have the necessary equipment to "bug" the office, "I know where I can get it."

As for the legality of overhearing the consultant's conversations, although several agents requested private meetings to discuss methods and price, only one of the investigators contacted frankly admitted the illegality of the proposed operation. He then indicated that many businesses had experienced problems similar to those voiced by the caller and had resorted to the same solution despite the prohibitions of Title III of the Federal Wiretap Act. He offered to discuss the possibilities further at a private meeting. Another investigator advised the caller that, assuming the caller owned everything in his office, "I believe you would be within your legal right" [to overhear the consultant's calls].*

In Baton Rouge, of nine firms contacted, five offered to perform debugging services, four would also conduct offensive wiretapping and bugging, and two others who did not offer offensive electronic surveillance themselves, referred the caller to an agency that did offer this service. When approached with the possibility of overhearing the consultants, one of the investigators hinted that this suggestion was "kinda on shaky ground, but it can be done." "We possibly could do something with his phone. If you own everything, that makes it better." Another suggested that a system "could be set up with a voice-activated tape recorder so that the slightest sound will start it." Another stated "we have various types of equipment. I feel sure we can

*As indicated above, several investigators concluded that the overhearing of the consultants would not be illegal if the caller (simulated employer) owned everything in the office. Section 2511(2)(a)(i) of Title 18 provides that it is not unlawful for the operator of a switchboard to intercept communications in the normal course of employment "while engaged in any activity which is a necessary incident to the protection of the rights or property of the carrier of such communication . . ." In conducting the survey, it was never indicated that the caller had his own switchboard. Had that been a fact, there would be some support for the view that monitoring of the telephone conversations of the consultants might not be unlawful. In *United States v. Christman*, 375 Fed. Sup. 1354 (1974), the court held that the defendant, regional chief of security for a department store chain, was not guilty of unlawful interception of telephone conversations when, having received reports of various improprieties occurring in the chain's shoe department, he monitored and recorded conversations occurring on the chain's *privately operated intercommunications system* (underscoring supplied). It is doubtful that this case correctly interprets Section 2511 (1)(a)(i). It is the position of the Department of Justice that the exceptions in 2511 (1)(a)(i) should be limited to the detection of telephone (toll) fraud and do not permit interceptions to gain evidence of other offenses of improprieties.

be of service." Finally, one agent assured the caller "anything you need in that line can be done. If it is illegal, we don't do it but we know who does and would be happy to talk to you about it."

Of 27 agencies contacted in Philadelphia, 20 provided debugging, 11 offered offensive wiretapping and bugging services, and three who did not perform offensive electronic surveillance themselves, referred the caller to agencies that would provide this service. One of the investigators suggested contacting the telephone company and having a monitor connected to the employer's telephone which would enable him to intercept all telephone calls to the office. Another stated, "there is a simple way to find out [about the consultants' outside activities]. Buy a small recorder. Can buy them in electronic stores. Get a long tape. Can plant in air conditioning duct, etc. There are devices you can pick up that are more sophisticated, but they cost more." He then explained that the caller could get in touch with an agency like "ours" which has this equipment, but it costs more. Another agent, when asked about the possibility of overhearing the consultants, stated, "I would prefer we discuss that when we meet." The caller asked, "I take it something can be done then?" The agent replied, "Yes."

Advice on the legality of the proposed "overhearing" varied. One advised the caller, "If you own the business you can do anything you want." He then indicated that his agency was "full up" and could not begin work on the caller's case for two weeks. Another, asked about overhearing conversations other than those taking place over the phone, said, "That can be done. You can put a device in there. I don't see anything illegal about that." Others were more cautious in their advice and actions. When asked about the possibility of listening to the consultants' conversations, two agents preferred to give advice and/or equipment to the caller rather than set up the monitoring system themselves. One stated, "Sure, I have the equipment and I can loan it to you. I can't do it. I can instruct you to do it." He suggested leasing the equipment at \$35-\$40 per week. The second replied that he could not do it but "I can tell you how to do it." He suggested that the caller place a tape recorder in the consultants' offices and run a line to wherever the caller would be so that he (the caller) could start and stop the recorder. Another investigator admitted, "It's illegal. If you do it on your own there is no problem." One agent advised the caller, "This could be done but you could not use the information—that would be eavesdropping." And another explained, "You can't use it [the information gained from the overhearing] for evidence. We can do it; there is no question about doing it. We have all the electronic equipment to do any job. It is against Federal law." He then asked the caller to come to his office in order to discuss the matter further.

Of nine agencies contacted in Washington, only two indicated that they provided offensive electronic surveillance and counter-measures. One of them suggested the use of a closed circuit TV that would allow the caller to monitor conversations while at the same time seeing everything that goes on from a car as far as one block away. The fee for this would be \$5,000 plus the cost of the operator if one were desired. As to the legality of overhearing the conversations, the agent stated that it would not be legal for him to listen in on conversations he was not a party to. He reported that he could make the equipment for the caller so that the caller could listen in. He advised the caller that although it would be questionable whether the caller could legally listen in on their conversations, the Courts would probably not say much unless some civil rights group took action. He emphasized that there would be no problem at all if the caller didn't tell anyone. The second investigator who was willing to provide offensive bugging and wiretapping services, indicated that legally the caller could tap his own phone but not the telephones of the consultants. He then asked to arrange a private meeting to discuss the possibilities further.

In Miami, of seven agencies contacted, four provided debugging services. Two indicated that they also provide offensive wiretapping and bugging, and a third indicated that his agency would do it if it could be done legally. To the suggestion of overhearing the consultants' conversations, the first investigator of this group responded, "Legally can be done if you own the office—I will not do it but I can offer advice. I can offer you assistance and show you how to do it." In reference to the necessary equipment, he offered, "I can get anything along that line that you need." Another investigator, asked about the feasibility and legality of the proposed overhearing, responded, "There are ways it can be done. You can [do it] for your own private information. I know it can be done. I have had it done." It was not clear whether one of the investigators who offered to perform offensive electronic surveillance would actually do so if he acquainted himself further with the law. When the proposal to listen to the consultants' conversations was brought forward, he responded, "There are a number of ways. I can take care of it. I won't do anything illegal; I am sure it can be done legally though."

In New York, of ten agencies contacted, one was strictly a guard agency and one was in the process of moving to another state. Of the remaining eight agencies, six conducted debugging operations and three offered to conduct or assist in conducting offensive eavesdropping activities. One of these agents stated, "You will have to install a listening device . . . have to set up a bugging system in the office. You could use a recorder." Another agent, when asked about overhearing the consultants, responded, "you can hear what goes on . . . We can do that." A third replied, "Setting up a device in the office is no problem at all." And the investigator from the agency preparing to move to another state commented, "I don't see anything wrong with that. They have some terrific mikes on the market today. [You] Can probably do it yourself. Get them at most any store—they don't ask questions. I used to do a lot of that when we were on (name) Street. I don't do it anymore."

Of 25 agencies contacted in Los Angeles, four were guard firms, one investigated fires only, and one performed property title searches only. Of the remaining 19 agencies, 16 were willing to conduct debugging searches, but none would provide offensive electronic surveillance services. However, three of the firms, after explaining that overhearing the consultants was illegal, suggested methods by which the caller might accomplish it. One agent commented, "It can be done. You may be able to buy your own [device] and get away with it. Some electronics companies will sell over the counter . . . \$1,000 to \$1,500. You may be able to find an agency that will do it for you." A second investigator suggested, "You could use a voice-activated tape that comes on automatically. Can be picked up at any store." A third agent advised the caller, "There's a place in Canada that will ship them in. They're expensive—\$1,000 to \$1,500. I can't recall the name though."

Telephone Company Data

On June 11, 1975, the American Telephone and Telegraph Company (AT&T) furnished the Commission with a list of the total number of wiretapping and eavesdropping devices found in the United States by Telephone Company personnel on the lines (facilities, equipment, and instruments) of the Associated Operating Companies of the Bell System during the period January 1, 1967, to December 31, 1974. The list (Exhibit No. 7.a.) reflects totals by year, and a breakdown by state.

On November 6, 1974, the Commission requested that AT&T provide additional data, namely, the type of illegal device discovered, the name, address and telephone number of the subscriber, the type of service—residential or business—and the law enforcement agency notified.

On January 13, 1975, AT&T responded to this request by furnishing the names of 1000 subscribers upon whose lines il-

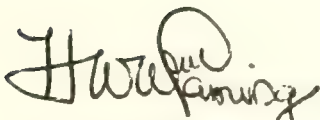
legal wiretap devices were found. (The list provided on June 11, 1975, indicates 1555 devices; however, AT&T records were not available for all the devices.) Exhibit No. 7.b. reflects a breakdown, by Associated Operating Companies, of the information.

The January 13 data submitted by AT&T shows that in 610 cases, the discovery of an illegal device was reported to the FBI.

On January 21, 1975, the Commission requested that the FBI provide information indicating the possible motives in each case, and the final disposition. Of the 610 cases, FBI records show receipt of only 473. Of these, 41 occurred prior to the enactment of Title III. A breakdown of the FBI response can be found in Exhibit No. 7.c.

TOTAL NUMBER OF WIRETAPPING AND EAVESDROPPING
DEVICES FOUND IN THE UNITED STATES BY TELEPHONE
COMPANY PERSONNEL ON THE LINES (FACILITIES,
EQUIPMENT, AND INSTRUMENTS) OF THE ASSOCIATED
COMPANIES OF THE BELL SYSTEM.

<u>YEAR</u>	<u>TOTAL</u>
1967	195
1968	179
1969	218
1970	195
1971	249
1972	174
1973	163
1974	182



H. W. William Canning
Attorney
American Telephone and Telegraph Company
June 11, 1975

TOTAL NUMBER OF WIRETAPPING AND EAVESDROPPING
DEVICES FOUND IN THE UNITED STATES BY TELEPHONE
COMPANY PERSONNEL ON THE LINES (FACILITIES,
EQUIPMENT, AND INSTRUMENTS) OF THE ASSOCIATED
COMPANIES OF THE BELL SYSTEM.

<u>STATE</u>	<u>1967</u>	<u>1968</u>	<u>1969</u>	<u>1970</u>	<u>1971</u>	<u>1972</u>	<u>1973</u>	<u>1974</u>
Alabama	5	2	7	9	7	13	6	12
Arizona	4	3	5	2	4	2	0	6
Arkansas	0	0	3	0	0	0	0	0
California	35	21	14	21	17	15	8	8
Colorado	1	4	3	2	1	2	0	3
Connecticut	2	0	1	5	2	5	1	0
Delaware	0	0	0	0	0	0	0	0
Florida	0	7	16	21	8	2	1	5
Georgia	2	4	1	7	2	11	4	6
Idaho	0	0	0	0	0	0	0	0
Illinois	15	17	31	15	55	26	12	20
Indiana	2	0	2	3	3	4	2	3
Iowa	0	2	0	0	0	1	1	1
Kansas	1	0	1	2	1	2	8	0
Kentucky	2	3	6	5	2	3	14	5
Louisiana	0	2	2	0	0	7	6	2
Maine	0	0	0	0	1	0	1	0
Maryland	1	3	1	2	4	3	1	3
Massachusetts	0	3	7	0	19	3	3	5
Michigan	24	17	11	6	29	6	1	3
Minnesota	1	2	0	0	1	2	5	2
Mississippi	2	2	1	1	6	1	1	2
Missouri	1	2	1	4	2	3	9	2
Montana	0	0	0	0	1	0	0	0
Nebraska	1	0	0	0	2	1	1	3
Nevada	2	0	3	0	1	0	0	0
New Hampshire	0	0	1	0	0	0	0	0
New Jersey	26	28	40	6	10	16	8	15

<u>STATE</u>	<u>1967</u>	<u>1968</u>	<u>1969</u>	<u>1970</u>	<u>1971</u>	<u>1972</u>	<u>1973</u>	<u>1974</u>
New Mexico	2	3	0	2	2	0	0	1
New York	0	0	1	5	5	5	10	6
North Carolina	3	3	1	6	4	3	4	1
North Dakota	0	0	0	0	0	0	0	0
Ohio	7	3	6	13	5	3	13	18
Oklahoma	0	0	0	0	0	0	0	0
Oregon	0	0	1	1	2	4	1	0
Pennsylvania	20	14	17	11	12	4	8	11
Rhode Island	0	0	1	0	0	0	0	0
South Carolina	0	5	3	3	8	5	7	3
South Dakota	0	0	0	1	0	0	2	0
Tennessee	14	8	10	6	13	4	0	8
Texas	13	16	9	18	9	9	4	11
Utah	1	3	1	3	1	3	0	1
Vermont	0	0	0	0	0	0	0	0
Virginia	0	0	1	2	4	2	6	3
Washington	6	1	2	5	4	2	4	9
Washington, D.C.	0	0	2	0	0	2	0	0
West Virginia	0	0	0	1	0	0	5	1
Wisconsin	2	1	6	7	2	0	6	3
Wyoming	0	0	0	0	0	0	0	0
TOTALS	195	179	218	195	249	174	163	182

EXHIBIT NO. 7.b.
 DATA CONCERNING ILLEGAL ELECTRONIC SURVEILLANCE DEVICES FOUND BY
 TELEPHONE COMPANY PERSONNEL ON THE LINES (FACILITIES, EQUIPMENT, AND INSTRUMENTS)
 OF ASSOCIATED COMPANIES OF THE BELL SYSTEM
 JANUARY 1, 1967 to JUNE 30, 1974

TELEPHONE COMPANY	NUMBER OF DEVICES FOUND	*CLASS OF SERVICE	**TYPE OF DEVICE	CASES REPORTED TO LAW ENFORCEMENT
New England Telephone Mass & Rhode Island	47	39 RES 7 BUS	6A 41C	45
New York Telephone	10	9 RES 1 BUS	6A 4C	10
New Jersey Bell	126	101 RES 22 BUS 1 Public Coin	40A 4B 81C 1D	122
Bell of Pa. Pa. & Delaware	45	36 RES 9 BUS	10A 1B 34C	39
C&P Company Wash., D. C.	2	1 RES 1 BUS	1A 1C	2
C&P of Maryland	27	19 RES 8 BUS	8A 18C 1D	20
C&P of Virginia	27	20 RES 7 BUS	7A 20C	15
C&P of W. Virginia	9	8 RES 1 BUS	2A 7C	8
Southern Bell Florida	74	57 RES 9 BUS	35A 39C	65
Southern Bell Georgia	50	48 RES 2 BUS	6A 44C	42
Southern Bell North Carolina	16	14 RES 2 BUS	4A 12C	14
Southern Bell South Carolina	32	28 RES 3 BUS	5A 27C	30
South Central Bell Alabama	40	34 RES 6 BUS	10A 30C	40
South Central Bell Kentucky	17	12 RES 5 BUS	9A 8C	17
South Central Bell Louisiana	22	14 RES 7 BUS	3A 19C	21
South Central Bell Mississippi	3	3 RES	1A 2C	3
South Central Bell Tennessee	56	52 RES 4 BUS	14A 5B 35C 2 Unknown	55
Ohio Bell & Cincinnati Bell	32	30 RES 2 BUS	3A 28C 1D	25
Michigan Bell	20	18 RES 2 BUS	2A 14C 4D	15
Indiana Bell	16	14 RES 2 BUS	6A 9C 1 Unknown	13

TELEPHONE COMPANY	NUMBER OF DEVICES FOUND	*CLASS OF SERVICE	**TYPE OF DEVICE	CASES REPORTED TO LAW ENFORCEMENT
Wisconsin Telephone	22	21 RES 1 BUS	8A 13C 1D	20
Illinois Bell	38	30 RES 8 BUS	27A 11C	0
Northwestern Bell Minnesota	10	8 RES 2 BUS	3A 7C	10
Northwestern Bell South & North Dakota	6	6 RES	6C	6
Northwestern Bell Nebraska	4	3 RES 1 BUS	1B 3C	4
Northwestern Bell Iowa	4	3 RES 1 BUS	2A 2C	3
Southwestern Bell Missouri	19	17 RES 2 BUS	1A 18C	16
Southwestern Bell Kansas	11	10 RES 1 BUS	1A 10C	11
Southwestern Bell Arkansas	3	2 RES 1 BUS	2A 1C	3
Southwestern Bell Oklahoma	3	2 RES 1 BUS	2A 1C	3
Southwestern Bell Texas	90	74 RES 16 BUS	31A 2B 54C 3D	75
Mountain Bell	0	0	0	0
Pacific N.W. Bell Washington	8	6 RES 2 BUS	4A 4C	8
Pacific N.W. Bell Oregon	7	6 RES 1 BUS	7C	7
Pacific Telephone Nevada	4	3 RES 1 BUS	1A 3C	4
Pacific Telephone California	100	77 RES 23 BUS	31A 3B 65C 1D	100
South New England Bell Connecticut	9	7 RES 2 BUS	4A 5C	6

TOTAL	1009	832 RES 163 BUS	295A 16B 683C 12D	877
		1 Public Coin	3 Unknown	

*Class of Service: RES - Residence, BUS - Business

**Type of Device: A - Radio Transmitted - Metallically coupled (Hardwire)
 B - Radio Transmitted - Inductively coupled (Transmissions picked up from magnetic field around wire)
 C - Metallically conducted (Transmits via hardwire) - Metallically coupled
 D - Metallically conducted - Inductively coupled

EXHIBIT No. 7.c.

DATA CONCERNING ILLEGAL ELECTRONIC SURVEILLANCE COMPLAINTS RECEIVED BY THE
F.B.I. FROM ASSOCIATED OPERATING COMPANIES OF THE BELL SYSTEM
JANUARY 1, 1974 to JUNE 30, 1974

MOTIVE

Disposition	Marital	Unknown	Domestic	Employee dis- honesty	Courtship Police (un- situation authorized)	Political	Industrial espionage	Business (fraud & internal problems)	** Other	Total
Number of cases	279	65	34	7	13	4	2	8	15	46
* U.S. Attorney declined prosecution	241	34	19	4	11	0	1	4	7	18
Handled by local authorities	7	1	4	0	1	1	0	0	1	0
Cases resulting in an arrest indictment and/or prosecution	13	1	1	3	1	1	1	1	3	2
Investigation discontinued	8	26	0	0	0	2	0	2	2	1
Investigation not conducted	5	2	9	0	0	0	0	0	0	0
No violation of Title III	4	1	1	0	0	0	0	1	2	24
Disposition unknown	1	0	0	0	0	0	0	0	0	1

* Reasons for declining prosecution include, lack of evidence, lack of prosecutive merit, a marital case with no professional interceptor involved, and expiration of the statute of limitations
** Includes cases involving theft of service, juvenile pranks, sexual curiosity, etc.
F B I inquires at various telephone companies established 22 cases which were reportedly referred to them but did not appear in F.B.I. records They are as follows 10 Marital, 4 Domestic, 1 Juvenile prank, 4 No violation, 1 in-
ternal business problem and 2 Unknown

COMPILATION OF NEWS ARTICLES ON ILLEGAL ELECTRONIC SURVEILLANCE

The staff of the National Wiretap Commission compiled several files of newspaper articles dealing with incidents of illegal wiretapping. A total of 304 reports of incidents have been collected, most of which deal with cases which occurred after 1968. Almost half of these cases involved allegations of illegal activities by state and local police, federal authorities, or other government officials. The rest of the cases involve the use of electronic surveillance by private individuals for a variety of purposes. Thirty-eight cases were selected as representative of those in the Commission's files and are summarized below.

ILLEGAL WIRETAPPING—POLICE

Paper:

Wichita Eagle & Beacon (Kansas)
1 Article, 5/23/75

Case:

Sedgwick County Sheriff & Deputies

Allegations:

Sheriff and deputy charged with illegal wiretapping, conspiracy to wiretap, and perjury. Gag order ruling prohibiting public comment by attorneys and witnesses involved in the case, which is pending. Trial set for June 17, 1975.

Paper:

Indianapolis Star (Indiana)
2 Articles, May 1975

Case:

Investigation of possible illegal wiretaps in police surveillance of Police Lt. John Wise.

Allegations:

Illegal wiretaps; some 25 tapes which may contain conversations recorded on basis of illegal taps were found in police "bug room;" secret surveillance equipment used to blackmail political figures; surveillance equipment is missing from police "bug room." Marion County Grand Jury investigation; tapes to be subpoenaed. Grand Jury investigation still in progress.

Paper:

Shreveport Journal (Louisiana)
2 Articles, April-May 1975

Case:

FBI Investigation of Capital Wiretaps

Allegations:

State police installed tap on Capital Police phones in February 1975, without a court order, apparently for internal investigative purposes; tap authorized by Captain Johnson of the Capital Police and State Superintendent of Buildings and Grounds Rizan; one witness claims police tapped illegally long before the Capital incident. FBI investigation. Still in progress.

Paper:

Manchester Union Leader (New Hampshire), 1 Article, 11/29/75
Orlando Sentinel Star (Florida), 2 Articles, 1/21/75, 1/29/75

Case:

Ficke Wiretapping Charges

Allegations:

Ficke, as Chief of Keene, New Hampshire Police Department, installed electronic interception equipment in his office that would intercept calls on an unlisted line. Specifically, he recorded a telephone conversation between a Keene police Sergeant and a city councilman and released information concerning the call to a radio newsman. Trial in Cheshire County

(N.H.) Superior Court. Ficke acquitted. Charges dismissed because state wiretapping law was too vague and no criminal intent proven. Ficke reinstated as Chief of Police, Winter Garden, Florida.

Paper:

Burlington Free Press (Vermont)
1 Article, 5/2/75

Case:

Scelza Suit

Allegations:

Scelzas charge their phone was monitored by the Hartford Police in connection with felony investigation. No charges were ever brought against any family member. Civil suit seeking injunction and \$200,000 in damages. Trial pending.

Paper:

Des Moines Register (Iowa), 5 Articles
Cedar Rapids Gazette (Iowa), 1 Article
7/18/74-3/18/75

Case:

Wiretaps in Cedar Rapids Police Station

Allegations:

Police bugged visitor and interrogation rooms, monitoring conversations between attorneys and their clients, generally in connection with lie detector examinations. Surveillance results also used in continuing investigations and gathering evidence. Equipment also used to monitor police officers. State and Federal Grand Jury investigations; National Wiretap Commission is considering a case study. State Grand Jury returned six indictments, which were dismissed on a legal technicality by the Iowa Supreme Court. They are currently reconsidering the matter. Federal Grand Jury produced a 500 word report concluding that illegal taps had occurred but that evidence as to responsibility was too skimpy to warrant indictments.

Paper:

Madison Times (Wisconsin), 2 Articles
Milwaukee Journal (Wisconsin), 1 Article
Memphis Commercial Appeal (Tennessee)
4/13/75-4/17/75

Case:

Wiretap Authorized during Indian Occupation of Alexian Brothers Novitiate

Allegations:

Tap illegal for failure to notify State Justice Department, although tap was authorized by Circuit Judge. No action taken; State A.G. announced that erroneous authorization and failure to follow proper procedures were not the intentional type of violation the law was meant to cover. Case dropped. It is possible that information gathered from the taps could be challenged successfully by the defense at trial of Indians.

Paper:

Nashville Banner (Tennessee), 1 Article, 5/1/75
Nashville Tennessean (Tennessee), 1 Article, 5/1/75

Case:

Vradenburg Stolen Gun Conspiracy

Allegations:

Vradenburg defense attorneys charged a government agent and a police officer with illegal tapping and with "setting up" burglaries to get evidence against the defendants. Grand Jury investigation. Acquitted; found "no creditable evidence of misconduct." Government agent promoted and transferred.

Paper:

Newark Star-Ledger (New Jersey), 1 Article, 3/25/75
Trenton Times (New Jersey), 1 Article, 3/25/75

Case:
New Jersey State Police Activities

Allegations:
Former state policeman charged that state police engaged in illegal wiretapping and in break-ins to plant bugs. State legislature's wiretap panel will hear testimony by ex-state trooper. Case pending.

Paper:
Hudson Record (New Jersey), 1 Article, 10/14/74

Case:
Hasbrouck Heights Council Report of Police Wiretaps

Allegations:
Former police chief secretly recorded conversations in his office and authorized taping of a closed police committee caucus meeting and a public meeting of the Borough Council. Investigation by Hackensack attorney and report to Hasbrouck Heights Council. Council read report at public meeting, but refused to actually release the report which concluded above allegations were true.

Paper:
Nashville Tennessean
2 Articles, 1/22/75 and 5/4/75

Case:
Suspensions of 3 policemen: Erwin, Prater & Bouchard.

Allegations:
Prater and Erwin illegally wiretapped the telephone of a suspected drug pusher. Bouchard suspended for waiting a year to report Prater and Erwin. Possible obstruction of justice charges. Federal Grand Jury investigation. Prater and Erwin reassigned to other duties in the police department; Bouchard reassigned; he resigned in March 1975 and is now suspected of involvement in illicit drug traffic.

Paper:
Chicago News (Illinois), 1 Article, 3/15/75
Chicago Sun-Times (Illinois), 1 Article, 3/15/75

Case:
Weiner Trial—Teamsters Union Defraud

Allegations:
Chicago police commander suspected of acting as middleman in arranging an illegal wiretap. Policeman gave a wiretap expert a \$2,200 check to arrange a wiretap on the home telephones of Weiner, who is on trial for embezzling \$1.4 million from Teamsters Union. Police department investigation. Pending.

Paper:
Chicago Tribune (Illinois), 1 Article, 1/29/75
Chicago Sun-Times (Illinois), 1 Article, 10/28/74

Case:
Illinois Bureau of Investigation's Illegal Taps

Allegations:
IBI engaged in illegal electronic eavesdropping in investigation of Jayne murder, investigation of the car bombing that injured State Representative Barr, and in other criminal investigations. FBI probe; Federal grand jury investigation; IBI internal probe. FBI probe established illegal tapping activities; findings turned over to U.S. Attorney who announced a grand jury would convene to investigate further. Glibbe, Superintendent of IBI fired from state job for failure to cooperate with IBI.

Paper:
Chicago Daily News (Illinois), 1 Article, 3/28/75
New York Times (New York), 1 Article, 3/30/75
Chicago Tribune (Illinois), 2 Articles, 3/31/75, 5/5/75

Case:
Police Wiretap on State's Attorney Bernard Carey

Allegations:
Chicago police accused of illegally monitoring State Attorney Carey's and Chicago Attorney Sear's telephones. Informants also alleged police kept surveillance on civic action and civil rights organizations. Police said to have developed equipment check-out procedures, whereby officers would check out equipment purportedly for use by civilian investigators in order to be shielded in case of grand jury inquiries. County grand jury convened; possibility of Federal inquiry. Investigations pending. Police superintendent tightening procedures for using surveillance equipment. Illinois Bell denies all allegations of their possible involvement.

Paper:
New York Times (New York), 2 Articles
Jamaica Long Island Press (New York), 1 Article
11/18/74-4/18/75

Case:
McClellan, Viera, Codelia Trails

Allegations:
Illegal installation of three wiretaps on the telephones of three narcotics-dealing suspects leading to shakedowns and acceptances of bribes to hinder the trials of suspects. Police detectives involved were indicted and tried (on taps and bribes, corruption). All three convicted; sentences pending. Two face possible 14-year sentences, third faces up to nine years.

Paper:
Los Angeles Herald Dispatch (California), 1 Article, 7/25/74

Case:
Lawton-Gardner Case (defendants in murder of policemen trial)

Allegations:
State used hidden bugging devices and hidden radio transmitters during the investigation of the case. Information disclosed during hearings held in preparation for third trial (previous two trials resulted in hung juries). Outcome pending.

Paper:
New York Times (New York), 1 Article, 3/6/75
New York Post (New York), 1 Article, 3/5/75

Case:
Rosenberg Raid

Allegations:
Three policemen accused of placing illegal wiretaps on telephone of college student suspected of drug pushing. They were also charged with depriving her of her constitutional rights and with stealing \$3,500 from her apartment during the 1970 raid. Detectives indicted on Federal criminal charges.

Paper:
Baltimore Sun (Maryland), 4 Articles, 2/5/75-3/28/75
Baltimore News-American (Maryland), 2 Articles, 3/6/75-3/14/75
Washington Star-News (Washington, D.C.), 1 Article, 2/2/75

Case:
Illegal Taps by Baltimore Police and the ISD

Allegations:
Police routinely placed illegal wiretaps on criminal suspects via vice squad officer and a contact in the telephone company. Police, Inspectional Services Division (ISD) and others accused also of monitoring politicians, labor organizations, reporters, and antiwar and civil rights protesters. County grand jury investigation of latter charge; Maryland State Senate Committee is holding investigative hearings on all illegal wiretapping activities. No indictments, reports as yet.

Paper:
Knickerbocker News (New York), 1 Article, 9/10/74

Case:
DiCocco Case

Allegations:
A legal stumbling block may impede solicitation of testimony from Paul (Legs) DiCocco in the Schenectady County grand jury investigation of organized crime. DiCocco was granted immunity by the jury but refused to answer questions on the ground that the inquiries were the product of an illegal wiretap. DiCocco's attorneys charged that DiCocco was not properly notified of the wiretapping after its termination. They obtained a show cause order in county court which bars the Organized Crime Task Force from asking questions which may be a product of the alleged illegal wiretaps pending the outcome of the order. A State Supreme Court rejection of the motion charging illegal wiretap evidence will be challenged by DiCocco's attorneys.

Paper:
Indianapolis Star (Indiana), 4 Articles, May 1975

Case:
Indianapolis Police Department—Illegal Taps

Allegations:
Former Police Chief Winston L. Churchill allegedly authorized special surveillances that led to illegal wiretaps of telephone conversations between a police officer and an Indianapolis madam. Results of the illegally monitored conversations were uncovered by Police Chief Hale as part of an investigation of police espionage. It was also disclosed that the Indianapolis Police Department sought unsuccessfully in 1971 to buy surveillance equipment, including some devices whose use would have been illegal even in police work. A Marion County grand jury has begun an investigation of alleged illegal wiretapping by policemen or outsiders working for the department. One such outsider, C. Tim Wilcox, president of International Investigators, Inc., was a consultant for the police department.

Paper:
Miami Herald (Florida), 1 Article, 5/22/75
Orlando Sentinel (Florida), 1 Article, 4/19/75

Case:
Florida Law Enforcement Commission

Allegations:
The Florida Department of Criminal Law Enforcement allegedly kept files on legislators and newsmen and engaged in illegal wiretapping. Special committees were appointed in both the Florida House and Senate to investigate the surveillance abuses.

Paper:
Pittsburgh Post Gazette (Pennsylvania), 2 Articles, 1/29/75, 1/30/74

Case:
Angelo Carcaci Testimony

Allegations:
The Pennsylvania House of Representatives ordered State Police Lieutenant Angelo Carcaci to appear before the full body to answer questions about a wiretapping investigation. Carcaci refused to answer questions during public hearings of the Committee to Investigate the Administration of Justice in the Commonwealth. The Committee was investigating the so-called King of Prussia affair in which one group of state troopers allegedly tapped the telephones of another state police unit assigned to the Pennsylvania Crime Commissioner investigating alleged police corruption in Philadelphia. For refusing to answer questions before the House, Carcaci was cited for contempt and imprisoned in a debate in which Republicans accused the Democratic administration of a cover-up of 1972 King of Prussia scandal.

Paper:
Philadelphia Bulletin (Pennsylvania), 1 Article, 5/15/75

Case:
Gerald Ewalt Suspension

Allegations:
Former Pennsylvania State Trooper, Gerald Ewalt, suspended from the force in 1973 as an aftermath of the King of Prussia wiretapping scandal, filed suit for reinstatement, back pay and punitive damages. Ewalt contends that he had no knowledge of the incident in which former State Police Commissioner Urella ordered taps on the phones of troopers investigating police corruption in Philadelphia. The affair led to the resignation of Rocco and the court martial of several officers engaged in the tapping.

Paper:
Shreveport Journal (Louisiana), 1 Article, 5/16/75

Case:
Baton Rouge State Capital Police

Allegations:
An incident in which Capital Police had a phone tap installed on their telephones is the subject of a major federal investigation here. The Chief of the Capital Security Force and the State Superintendent of Buildings and Grounds admitted that they had requested the taps from state police without a court order. The taps were allegedly designed to intercept a caller who threatened the life of a Capital policeman. Charges that Capital Police Chief Johnson monitored calls months before the state police installed taps are also under investigation. The bugged lines were probably used by officers who were not told of the wiretaps, making the taps illegal.

ILLEGAL WIRETAPPING—PRIVATE

Paper:
Desert News (Utah), 1 Article, 11/20/74
Cincinnati Enquirer (Ohio), 1 Article, 5/16/74

Case:
Merrill Bean Chevrolet Case

Allegations:
Merrill Bean Chevrolet was indicted by a Federal grand jury in October 1974 for allegedly violating Federal wiretap laws by monitoring conversations between customers and employees with two-way speakers in an effort to increase car sales. FBI agents confiscated 16 electronic bugs from the dealership last May. A U.S. District Judge heard the case.

Paper:
Salt Lake City Tribune (Utah), 1 Article, 5/6/75

Case:
Brigham Young University—Latter Day Saints

Allegations:
The FBI concluded its investigations of charges that Brigham Young University Security Police violated Federal wiretapping laws after finding no evidence of any wrongdoing. Allegations of interceptions of conversations used in LDS excommunication proceedings were also dismissed by the FBI as unfounded. The FBI, however, did caution LDS leaders after an incident.

Paper:
Bridgeport Post (Connecticut), 1 Article, 5/8/75

Case: Illegal Taps—John Norton Case

Allegations:
A Federal District Court Judge dismissed all charges against John Norton, a Fairfield lawyer and trial judge, stemming from an indictment for wiretapping his own drugstore. Norton wished to look into the activities of some of his employees at his Washington drugstore, but his wiretapping devices were discovered by the telephone company. The Justice Depart-

ment moved for dismissal of all charges although the case against Norton's partner in the wiretapping scheme, a New York private investigator, is still pending.

Paper:

San Jose News (California), 2 Articles, 4/22/75, 5/13/75

Case:

Richard Ruth Case

Allegations:

A San Jose private investigator has been charged with violations of Federal wiretap laws stemming from his visit to the scene of a murder. Ruth was reportedly summoned by the murder suspect and declined to answer police questions. Hoping to find the murder weapon, police obtained a warrant to search Ruth's home and discovered wiretap equipment, burglary tools and tapes of phone conversations.

Paper:

San Jose Mercury (California), 1 Article, 1/19/75

Case:

Hal Rogers Case

Allegations:

Hal Rogers, president of Taxpayers Unanimous, lost his invasion of privacy suit against the City of San Jose and its information officer, Robert Ulrich, in which Rogers charged that Ulrich had illegally tape-recorded a conversation between himself and Ulrich. Ulrich phoned Rogers to inform him that his organization could not meet in city council chambers. Rogers filed an immediate appeal.

Paper:

Vincennes Sun-Commercial (Indiana)
New York Times
January 1975

Allegations:

The Indiana Bell Telephone Company is investigating possible illegal wiretaps on three telephone lines of the National Clemency Information Center. The center, sponsored jointly by a unit of the National Council of Churches and the American Civil Liberties Union, counsels military deserters. The Center brought a suit in December 1974 against Secretary of Defense Schlesinger and others alleging that the amnesty program is unconstitutional.

Paper:

Newsday (New York), 1 Article, 5/6/75

Case:

Bugging in Washington

Allegations:

Why are so few bugs discovered in Washington, a city said to fear the widespread use of eavesdropping devices? One reason, according to some sources, is that there aren't as many bugs as people seem to think. This is because the 1968 Omnibus Crime Control Act, which imposes penalties for willful eavesdropping done without a court order, has made bugging more expensive. Another explanation for the lack of "finds" is the widespread ignorance of the illegality of eavesdropping which exists. Finally, those who discover bugging devices tend to keep quiet. Disclosure might unnecessarily tip a hand, jeopardize a relationship with a client, or involve one in a law suit.

Paper:

Chicago Tribune (Illinois), 1 Article, 5/5/75

Case:

Illinois Bell Telephone

Allegations:

Illinois Bell Telephone stated that it opposes wiretapping and would refuse any requests by the Chicago Police Department to assist it in wiretapping. The statement came in response to reports that unnamed telephone employees were coerced into wiretapping by Chicago police and an unnamed alderman. Illinois Bell insisted that it would take disciplinary action if any employees were found guilty.

Paper:

Kansas City Star (Missouri), 1 Article, 4/16/75

Case:

Robert B. Heinen

Allegations:

The FBI is conducting an investigation of an alleged wiretap placed on the phone of Robert B. Heinen, a former police captain who now heads the International Bureau of Investigation, a private investigation agency. Heinen has been a persistent critic of Kansas City Police Chief Joseph D. McNamara and is currently involved in a second legal attempt to challenge McNamara's qualifications to be chief. Police denied any knowledge of Heinen's complaint or the device found attached to his phone line.

Paper:

New York Times (New York), 1 Article, 3/20/75

Case:

Richard Geyer Case

Allegations:

Richard Geyer, a Florida private detective who distributes electronic surveillance equipment to numerous law enforcement agencies, was charged with having bugged a New York hotel room occupied by a broker for Lloyd's of London. Geyer claimed that he was only testing the equipment for a potential customer, but industrial espionage against potential clients of Lloyd's may have been a possible motive. The FBI charged Geyer, president of the Tracer Co., and Dale Tolbert, chief pilot for Surety Industries, with illegal eavesdropping.

Paper:

New York Times (New York), 1 Article, 10/28/74

Case:

Kuh-Morgenthau Race for Manhattan District Attorney

Allegations:

Richard H. Kuh, the Manhattan District Attorney, charged that his Democratic opponent, Robert M. Morgenthau, hired a private detective in 1955 on behalf of the Panhandle Eastern Pipeline Corporation of Houston to illegally tap the phone of a Panhandle competitor. Kuh urged that Mr. Morgenthau consent to an inspection of the files of Robert Maheu, the private investigator allegedly hired by Morgenthau and who is now known as a Howard Hughes associate. Morgenthau could not be reached for comment.

Paper:

New York Times (New York), 1 Article, 9/25/74

Case:

Mafia Taps Mafia

Allegations:

Organized crime members have been wiretapping the telephones of their enemies illegally in attempts to gain the advantage in the current mob wars, Brooklyn District Attorney Eugene Gold said. Mr. Gold stated that a telephone company employee, Paul Mess, and James Geritano, a reputed member of the Gallo family, were indicted for allegedly tapping the phone of Gennaro Basciano, a member of a breakaway faction of the Gallo mob.

Paper:

New York Daily News (New York), 1 Article, 8/8/74
Philadelphia Inquirer (Pennsylvania), 1 Article, 8/8/74

Case:

Conspiracy to Disrupt Trials of DiGilio and Valvano, in New Jersey, on Loansharking Charges

Allegations:

Ten persons were charged inter alia, with planting electronic devices in defense attorneys' offices. Conspirators also accused of trying to place blame for illegal bugs on federal agents in attempt to get DiGilio, Valvano charges dismissed. Ten persons involved were indicted on charges of conspiracy, obstructing justice and planting the wiretaps. Outcome unknown.

Paper:

Law Enforcement Journal, 1 Article, May 1975

Case:

Illegal Taps—Quartermain Case

Allegations:

Quartermain, a private detective in England, pleaded guilty to charges involving conspiracy to trick government officials and police departments to divulge confidential information and perverting justice by constructing false evidence. Quartermain was sentenced to three years' imprisonment and fined 500 pounds.

CHAIRMAN ERICKSON: Joseph Jaffe.

[Whereupon, Joseph Jaffe was sworn by Chairman Erickson.]

TESTIMONY OF JOSEPH JAFFE, ASSISTANT UNITED STATES ATTORNEY, SOUTHERN DISTRICT OF NEW YORK

CHAIRMAN ERICKSON: Joseph Jaffe, Assistant U. S. Attorney for the Southern District of New York. Mr. Jaffe has held that position since September of 1971, and since April of 1974 has been the Chief of the Official Corruption Unit in the Office of the U. S. Attorney.

Mr. Jaffe is here to discuss the allegations of illegal police wiretaps from 1968 to 1971, which outline federal involvement in prosecution of the wiretap charges.

Do you have an opening statement, Mr. Jaffe?

MR. JAFFE: Mr. Chairman, I have an opening statement which encompasses three additional areas in addition to the areas you pointed out. If the Commission desires, I will read the statement in its entirety or confine it solely to the area of the illegal police wiretapping.

CHAIRMAN ERICKSON: We would welcome the filing of the entire statement, if you have no objection to that. It can be made part of the record for the purpose of further study of the Commission and use in the Commission's report.

So if you would be willing to file that report and could give a summary of the report, we could proceed with our examination.

MR. JAFFE: That is quite all right with me, sir. I have sent a copy to Mr. Butler and to Mr. Hershman, and I believe they have additional copies, so I could just answer whatever questions you desire.

CHAIRMAN ERICKSON: If you would make a summary of it, I think it would be well for the record.

[The prepared statement of Joseph Jaffe follows.]

STATEMENT OF JOSEPH JAFFE, ASSISTANT UNITED STATES ATTORNEY IN THE OFFICE OF PAUL J. CURRAN, UNITED STATES ATTORNEY FOR THE SOUTHERN DISTRICT OF NEW YORK

The following statement is prepared in response to the questions posed in the Commission's letter of May 20, 1975.

I. *"The difficulties, if any, in prosecuting cases of illegal electronic surveillance under current Federal statute."*

The difficulties in prosecuting illegal electronic surveillance cases often depend on whether the subjects are law enforcement officials or private individuals. With regard to the prosecution of law enforcement officials the difficulty lies not so much with the statutory scheme but with the detection of illegal electronic surveillance. Where law enforcement personnel have obtained a court order or have made disclosure as to the existence of electronic surveillance the problem is somewhat easier. However, the most difficult problem in both the law enforcement sector and in the private sector is that most frequently the illegal use of electronic surveillance cannot be detected.

The basic reason is twofold. Number one, usually there is no information available because either the law enforcement officials or the private sector individuals have not applied for any court orders. Number two, there does not appear to be any central registry of available electronic surveillance equipment. This is more true in the private sector than in the public. Given the abundance of such equipment, to which both law enforcement and private sector people have easy access, and since few if any records are kept of persons selling, buying or renting such equipment, their activities remain undetected. Detection and prosecution thus remains impossible. The statutory scheme as it is setup on its face is broad enough to cover any detected instances of the use or abuse of electronic surveillance. In short the problem is mainly one of detection, not prosecution once discovered!

II. *"The difficulties, if any, in interpreting those statutes, and recommendations for possible changes."*

The main difficulty in interpreting the statutes as they exist is to distinguish between those cases where the use of electronic surveillance is clearly barred by statute, for example, where no court order is obtained and those areas where a court order is obtained and either (a) the underlying papers are deficient and fail to state sufficient probable cause or (b) the conduct of the surveillance is not within the prescribed limits, for example, individuals involved have failed to minimize the conversations or they have failed to warehouse the tapes as they are required to do. We are familiar with cases where a joint federal-state prosecution was based, in part, on electronic surveillance authorized by a state court where because of either a lapse in obtaining a renewal of the state order so that the intervening conversations become illegally obtained, or because of a failure by the officers to minimize the conversations, the conversations obtained were held to be illegally seized within the meaning of

the Fourth Amendment and the wiretap statutes as interpreted by various federal courts. Clearly federal and state prosecuting authorities in such situations are barred from using such materials or the fruit of such materials as evidence at a trial or in a prosecution. However, having attempted to comply with the statutory provisions it seems clear that the officers involved have not committed any intentional or criminally motivated statutory violation. While that is not absolutely clear, given the present statutory language, it seems that there have been no prosecutions for such violation nor should there be any unless the officers purposefully attempted to wilfully circumvent the statutory requirements.

Another problem exists within the statutory scheme. Sections 2511 and 2512 appear to bar all but authorized law enforcement personnel or persons involved in common carrier communications from obtaining or using surveillance equipment. However, Section 2511(d) allows any person who is a party to a conversation to participate in a consent interception of that conversation. Given this section and given the unregulated distribution of surveillance equipment purportedly for this purpose, that is, consent interception, it appears that Section 2511(d) is the loophole which permits much of the industrial espionage in existence today to be conducted and allows it to survive.

It would seem that that section could be limited to use of telephone surveillance equipment which a consenting party could attach or have attached by common carrier. Moreover, the unregulated manufacture and sale of bugging equipment still seems prevalent. This allows private detectives and persons in industry access to wiretapping and bugging equipment. All of this could be at least somewhat curtailed under the present statute by stricter regulation and enforcement rather than by statutory change.

III. *"Details of the prosecution of police officers formerly assigned to the New York City Police Department's Special Investigations Unit on charges of illegal electronic surveillance."*

The United States Attorney's Office for the Southern District of New York, in conjunction with the United States Attorney's Office for the Eastern District of New York, and agents assigned to the Drug Enforcement Administration, together with officers assigned to the New York City Police Department, First Deputy Commissioner's Special Force commenced a series of prosecutions culminating in the indictment and conviction of more than twenty then present and former members of the "elite" Special Investigations Unit, Narcotics Bureau, New York City Police Department.

This unit in 1969 through 1971 was responsible for the apprehension and seizure of hundreds and hundreds of pounds of heroin and cocaine that had been illegally brought into the United States. The officers had a reputation for making the most significant narcotics cases. Ultimately, of course, they also had a reputation for stealing huge amounts of money. In fact, two of them have been convicted of stealing and selling more than 5 kilograms of heroin and cocaine themselves, narcotics which they seized from South American importers. Few of these individuals have been charged with the specific crime of violation of the electronic surveillance provisions of Title 18. However, the evidence presented at the trials of a number of these indicted officers disclosed a pattern of illegally obtaining evidence, illegally arresting narcotics offenders, taking their money and thereafter releasing the offenders.

Other information made public at various trials and hearings in connection with the prosecution of other officers, narcotics offenders or lawyers representing them, established that the overall pattern used by the S.I.U. was based in large measure on the use of illegal electronic surveillance. Given the nature of the charges to which the officers ultimately pleaded guilty or on which they were convicted, which were much more serious charges and also were much more triable in terms of jury appeal,

only a few police officers have been charged with participating in illegal electronic surveillance. From the evidence now public the picture that emerges is that from the period of at least 1969 through 1970 it was routine for the police officers charged with narcotics enforcement in the major drug cases in the City of New York, S.I.U., to routinely use illegal electronic surveillance.

Some witnesses have testified in fact that the regular pattern was once a person was suspected of being a narcotics offender, that person would be placed under illegal electronic surveillance which would include: wiretapping any telephones regularly used by the subject, bugging any apartments or houses used by the subject, bugging automobiles used by the subject. The evidence also disclosed that even in the cases where court ordered wiretaps were obtained on particular locations, (for example, in the 14th Street area of Manhattan, which was notorious as a meeting ground for South American drug dealers in 1969 and 1970, a court ordered wiretap was obtained for one public telephone in a meeting place called the Cafe Madrid) the S.I.U. officers would not only wiretap the telephone ordered to be tapped by the court, but would wiretap the other telephones without a court order, to obtain narcotics information. Once the officers illegally obtained the information they would, in some instances, follow up by making arrests, seizing narcotics and prosecuting the offenders based on the illegal information. The papers filed with the court, however, would never indicate the true source of the information but would be disguised by attributing the information to fictitious "confidential informants." In many instances, however, the officers would not make any arrests, seemingly legitimate or otherwise, but would merely find and detain narcotics offenders, steal their money, sometimes ranging up to the hundreds of thousands of dollars, and thereafter release the offenders. In many of the cases investigated by the United States Attorney's Office for the Southern District of New York of S.I.U. officers the evidence showed that the police officers involved obtained their leads and in fact the identities and locations of narcotics offenders through the use of illegal electronic surveillance, most of which was never court authorized.

In other cases about which I cannot further comment, it was established that for no illegal motive, but merely for the motive of obtaining arrests and convictions of narcotics offenders many S.I.U. officers did the same thing. As a result of these investigations a number of convictions in state court, even though they were convictions based on guilty pleas, some after suppression hearings, have had to be set aside and the narcotics offenders freed.

In part, some of the fault may be attributed to overzealous narcotics enforcement officers, in part some of the blame lies with the Police Department superstructure which permitted such overzealousness to exist. However another contributing cause was the attitude of several Assistant District Attorneys in the state system who if not overtly at least covertly encouraged such illegal activity. And, in part, the blame lies with the education of the American public, which does not yet understand that the constitutional system that we have does not allow the ends sought to justify the means used. This matter of education is one about which, perhaps, this Commission could be of help. Until the American public understands that the Government or the people have the burden of proving the guilt of a defendant by legitimate, constitutionally approved methods, until the police are also so educated, and until the American people or the people in a particular city are made to understand that because a person is a bad person that does not justify use of illegal means to capture or prosecute him, then all the laws on wiretapping, all the laws on search and seizure, all the laws on presumption of innocence, in fact the whole justice system will continue to be "shocked" by the revelations of the illegal activities of the kind we discovered during the course of our investigations. I will not dwell on the particular facts of any particular situation unless the Commission has specific questions.

IV. *"Views as to the viability of using independent investigators to investigate allegations of illegal police wiretapping."*

The question as to viability of using independent investigators other than for example, the F.B.I., as suggested by the Commission's letter of May 20, 1975, really begs the question of adequate enforcement of the current wiretapping and eavesdropping provisions of the United States Code. In the Southern District of New York, to my knowledge, the F.B.I. has made few wiretapping or bugging cases. The few cases that we now have pending in our District were cases forwarded to them by our office. That, however, should not be taken as a criticism of the F.B.I. in terms of their ability to make wiretapping cases. The problem is, from our point of view, that there are only so many things any federal investigator can investigate at a particular time. A determination has to be made as to the priority to be placed on specific investigations or prosecutions. Without adequate manpower, without adequate funds, without adequate equipment, whether an investigator be an "independent investigator" or an F.B.I. agent, or a D.E.A. agent or a Customs agent or an I.N.S. agent, or an I.R.S. Special Agent or Inspector, or a Postal Inspector or any of the other law enforcement officers that have jurisdiction to investigate any federal or state crimes, he cannot do so because all of these agencies are understaffed, underpaid, underequipped.

An analogy might be made to the area of gun control enforcement. Without expressing any views as to the gun control laws it would seem that if the Bureau of Alcohol, Tobacco and Firearms was given more manpower and more money so that there was time to investigate all the crimes within that Bureau's jurisdiction, the gun control laws would be more effectively enforced. Similarly, were the United States Attorney's Office for the Southern District of New York or any other United States Attorney's Office to have the manpower available such that it could focus on the illegal eavesdropping problems through its own investigators or through any other agencies who would have the additional investigators, then prosecutions could increase.

The fact that the F.B.I. works closely with local law enforcement officials should not be taken as any conclusive ground to show that the F.B.I. could not investigate illegal activities of law enforcement officials who might be involved in illegal electronic surveillance activities. If that were the case then I suppose we should do away with all the inspection or integrity services and all the federal enforcement agencies because everyone of them does or should work closely with local law enforcement. Thus the answer is not necessarily "only independent investigators" which, of course, would help our office in not just illegal electronic surveillance cases, but all cases. Rather, the answer is especially more manpower and equipment to do a more adequate law enforcement job.

MR. JAFFE: I think the area it would be best for me to comment on, Mr. Chairman, would be to give a summary of what was known as the Special Investigation Unit, known as the SIU, the elite narcotics group in the New York City Police Force.

To capsulize the statement and capsulize our experience with it, the SIU was for a number of years, specifically from 1969 through 1971, a group of approximately 50 to 70 police officers of detective rank or above, although some were of police officer rank.

The SIU was charged by the city police department with the investigation of major narcotics cases. The men assigned in that unit worked in

groups usually of four to six men. Six to seven groups would be assigned to a sergeant. The commanding officer was a lieutenant. For the most part, that lieutenant was John Egan, and there was a captain above Egan. The names of the captains changed during that period of time.

The experience we uncovered with that particular group was that although these police officers made substantial arrests and substantial seizures of narcotics on individual occasions amounting up to in excess of 100 kilos of narcotics at a time, this particular group of individuals also stole hundreds of thousands of dollars from the narcotics offenders that they were charged with prosecuting. And our experience was that for the most part the narcotics offenders were detected, arrested, or stopped, based on information that had been gathered through illegal electronic surveillance, both illegal bugging and illegal wiretapping.

There was, in fact, a standard procedure—and I can say to you, ladies and gentlemen, that the information I give to you for the most part is public record. It has been testified to in more than seven trials. Our office, together with a number of other offices last year—in February of last year—initiated an investigation into the SIU. That investigation—and I bring this up because of some of the things I have heard other witnesses say today—was conducted jointly with another United States Attorney's office, with a special group of New York City police officers assigned to what is called the First Deputy Commissioner's Special Force.

That group, together with our office and another United States Attorney's office, together with special agents assigned to the Drug Enforcement Administration and special agents assigned to the Internal Revenue Service, conducted an investigation that ultimately led to the indictment and conviction thus far of more than 25 members of the SIU, including the commanding officer, Egan.

Two officers of the SIU we have prosecuted for stealing and selling more than 5 kilograms of heroin and cocaine.

I can give you details of those as the questioning comes up.

But in the process of the investigations, both in the prosecution of the cases I have just spoken about and in continuing investigations and hearings which were connected to prosecutions of attorneys and other police officers, the standard practice that we found to exist in New York City in narcotics enforcement from 1969 through '71 was that routinely when SIU investigators—detectives or sergeants or whatever—suspected an individual of being a narcotics trafficker, they would set up a surveillance, and that surveillance would include wire-

tapping any telephones that the suspect would use; bugging any apartments or houses that the person frequented or lived in; bugging the automobiles that the suspect would use.

In some cases the police officers would obtain court-ordered wiretaps. Even in the cases—and I don't say this happened in every case, but in a lot of the cases we were familiar with—even if there was a court-ordered wiretap for a particular installation—for example, in this period of time we are speaking about, the major importers of heroin and cocaine in the New York City area were South American individuals. Those individuals frequented two areas of New York City. One was the 14th Street area; the other was the Broadway and 72nd Street area.

A particular example that would interest the Commission: There was a place called the Cafe Madrid where a lot of narcotics business was transacted. A court-ordered wiretap was secured on the Cafe Madrid for one telephone. The SIU officers put in taps on all the telephones in the Cafe Madrid. There was no minimization. There was constant 24-hour monitoring of all the telephones.

That is an example. And if we review some of the cases during the questioning, I will point out to you that quite often to secure the court-ordered wiretaps or to secure search warrants or arrest warrants, the person who would be identified in the affidavit as a confidential informant who had previously provided reliable information was not an informant at all. That person was either a bugging device or a wiretap which was non-court-ordered.

What we found in our investigation was that there were a number of officers who used this illegal electronic surveillance in order to secure arrests and seize large quantities of narcotics. Perhaps that is an excusable thing to do.

What we also found, however, was that once that illegality began, it never ceased, because the people that we indicted and convicted or whom we indicted and people pleaded guilty, once they began to obtain the illegal information, their justification—well, I am jumping ahead of myself.

Once they began to use these illegal devices, they had to pay for them. The New York City Police Department at that time did not have substantial money available to either make undercover business or to provide a lot of equipment. The officers would buy a lot of equipment. Some of it was purchased from persons whom your investigators are familiar with.

That equipment cost an awful lot of money. And so to pay for the investigation, when a narcotics offender was arrested, if he had quantities of money on him, instead of vouchering the money, the of-

ficers would take what they felt was fair compensation for the money spent on an investigation, and either at that time or very soon thereafter, it wasn't too long a jump before the officers began to just take the money and put it in their pockets.

And with regard to certain officers, they began to steal not just hundreds and not just thousands, but literally hundreds of thousands of dollars. And it wasn't long after that, or at the same time, that the officers also needed excuses for arresting people. That is called flaking.

And in the trial I completed just about two weeks ago there was an awful lot of testimony about flaking. What it simply means is if you don't have enough to arrest a man, you put the evidence on him and then you arrest him.

Sometimes the narcotics officers did that with weapons in order to secure an arrest and thereafter seize quantities of narcotics, and often they also did it with quantities of narcotics. And they had to have a source for their narcotics. And the source of their narcotics was the narcotics that they would seize and fail to turn in to the police department.

Having gone that far, it wasn't too long a step for two officers who we have indicted and convicted—and there were others who were involved—to partake in a tremendous drug seizure and steal the narcotics.

In a case we just finished trying—we tried it once before—the defendant was a fugitive in Ireland until we got him back in May. We tried it last year when we had his partner in custody. The officers were involved in what has been called the largest domestic drug seizure in the United States, or at least in the Northeast area. In part, that investigation was based on illegal wiretaps.

They seized four individuals, and after the four individuals were persuaded—and we can go into the details if you want—to give up the location of the narcotics, the officers went to the apartment and found 105 kilograms of heroin and cocaine. They kept five and vouchered the rest in, and then they sold it.

I bring this out not particularly because it is a matter of illegal wiretapping. We have a lot of other cases I can discuss where the wiretapping led to the seizure of over \$250,000. But I bring it up because I think it is important for the Commission as part of its function to help educate the American people.

I bring it up also because that education is necessary in order for the Commission or for any prosecutor to have successful wiretap prosecutions.

Many of the men that we have arrested and have convicted, either by plea or by trial, could have been charged with illegal wiretapping in addition to obstruction of justice, facilitating the sale of nar-

cotics, and sale of narcotics. In the Eastern District there were some charges of civil rights violations.

But to specifically charge a police officer with illegal wiretapping in the circumstances where the individual who he arrested is a bad person in the public's view and the police officer made no money or private gain on it makes it a case that has no jury appeal because the jury and the American public doesn't understand—and I said it in the outline and say it again here as strongly as I can and hope the Commission would do the same—the American public doesn't appreciate our constitutional system.

The Constitution says the government—or the people if it is a state or a commonwealth—have the burden of proving guilt by following certain constitutional and legal standards. The American public doesn't understand that. The American public believes for the most part that if a man is a bad man, the ends can always justify the means used. And while that may have some appeal, that is not our law and it is not our Constitution, and unless we educate the public and thereafter educate the police departments and police chiefs and the mayors and the district attorneys, we won't change that system.

That brings me to another point, and that is with regard to the SIU cases. How do you ascribe blame when you understand that out of 70-some people or at the most 90-some people in a particular year, from the testimony that was given, the most that people would say is that perhaps two of the 70 or 90 didn't take money, didn't illegally wiretap, didn't pocket or profit at the expense of the people they were investigating?

You cannot conclude that the Police Department of the City of New York assembled the 90 or 70 or 50, whatever year you are talking about, of the biggest thieves and most corrupt police officers and put them into one unit. What you have to do is look at the police officers and the pressure they are under. You have to look at the over-zealousness which they had to have to get a lot of poison off the street. So you can't be Solomon-like and say only the police officers are involved.

Part of the blame has to be given to the police department for not policing the people that they were supposed to.

That goes to what some of the testimony was before from one of the witnesses about who looks at the police department. You can look at your own to a limited extent, but you'd better have an integrity unit to do that looking also.

But part of the blame, if we are going to ascribe blame, also has to go to some of the assistant district attorneys in the New York City area and the law enforcement officials in general who, if not overtly, at least covertly, went along with the idea.

You have to put part of the blame on the assistant district attorneys and on the law enforcement officials who, if not overtly, at least covertly, went along with the idea you could use illegal wiretapping and illegal bugging in order to get the necessary probable cause to thereafter get either the legal bug, the legal wire, or the legal search warrant.

And as I say, I think it is an educating function that this Commission could help with tremendously. It also explains, from a prosecutor's point of view, why it is that prosecuting a wiretap case on its own with nothing else is very difficult.

Now, gentlemen, and Mrs. Shientag, I didn't mean to just say gentlemen—

MS. SHIENTAG: That's all right. I'm one of the boys.

MR. JAFFE: That is a summary of what is in the statement, and since you have the statement I will not say anything further and just open it up to any questions that you have.

CHAIRMAN ERICKSON: Mr. Hershman.

MR. HERSHMAN: Thank you, Mr. Jaffe. I think if you were to say nothing further, the Commission would still be immeasurably helped by the testimony you just gave.

Can you tell us how pervasive the wiretapping was in the unit? You said the unit ran perhaps 70 officers. Do you have any idea how many were using wiretapping at one time or another?

MR. JAFFE: From the testimony we had and the information that is either public or can be made public, we are informed that with regard to the Special Investigations Unit, it was the normal practice to illegally wiretap and illegally electronically surveil any major narcotics offender or subject who was considered so.

MR. HERSHMAN: I assume, then, they all knew how to do this; is that correct?

MR. JAFFE: From the information that we have, of the teams that were in existence, if not every person on the team at least a good number on the team knew how to install the electronic devices.

I might point out also that there were people who were involved in SIU who were, for example, involved in monitoring, who would be misled by some of their brother officers and told the tap was legal and they did not ask, they did not inquire further.

MR. HERSHMAN: You stated earlier that these police officers often paid, from their own pocket, money to purchase electronic surveillance equipment.

MR. JAFFE: That is correct.

MR. HERSHMAN: I assume this was done without the knowledge of their superiors within the New York City Police Department but outside of the SIU.

MR. JAFFE: If I understand your question correctly, it was done with the knowledge of the superior officers within the SIU. Whether or not the superior officers outside the SIU knew about it, we cannot prove that they knew about it. We can make assumptions that they probably should have or did in fact, but it is hard to prove that the superiors who weren't in direct contact actually knew about it.

MR. HERSHMAN: Well, there were no vouchers or LEAA funds to purchase this equipment, were there?

MR. JAFFE: No. One source of that equipment, who I know, Mr. Hershman, you are familiar with—whether or not he gave vouchers I don't know. But no, the equipment was bought and paid for by the police officers, we were told, with cash, and when they felt the investigation was concluded they'd reimburse themselves.

MR. HERSHMAN: It is my understanding they purchased equipment merely on showing their shields or their badges. Is that your understanding, sir?

MR. JAFFE: I don't know that they even had to go that far. I know that there were particular electronics manufacturers, and I don't think they were any of the large firms, some of whom you had testimony on here. I think they were people who ran their own shops, who could make almost any type of equipment. With regard to the tape recorders and things like that they needed, they could purchase them anywhere.

MR. HERSHMAN: So there was never a lack of equipment?

MR. JAFFE: No. As we and the juries and judges who heard the cases were told, there may have been a lack of equipment from police department authorized sources, but there was no lack of equipment in order to pursue these investigations.

MR. HERSHMAN: One former member of the SIU unit who has been indicted stated that approximately 90 per cent of the court orders sought by that unit were based on affidavits stating "confidential informants," when, in effect, the information came from an illegal wiretap. Would you say that is a correct figure?

MR. JAFFE: From the testimony we have heard in the investigations we have done, for the years involved, which would be '69 through '71, the information supports that, that is, that most of the affidavits were, at least in part, based on illegally obtained evidence, either through wiretap or eavesdropping or from other methods, for example, breaking into rooms or things of that nature.

Whether or not that witness or any of the other witnesses who have testified are exaggerating, we

don't know how to test. We do know that in cases we were involved in investigating, one of the results of our investigation was that people who had been indicted in various counties in the New York City area, who had had suppression hearings which were denied, thereafter pleaded guilty and were sentenced to somewhat substantial terms in jail.

One individual, Legusman, for example, I think had been serving a 14-year sentence. As a result of our investigations, the cases against those people which were in state court were dismissed, and the people were released from jail.

MR. HERSHMAN: Are there other cases like that?

MR. JAFFE: There are a number of cases where individuals have either been released from jail or the prosecutions which were pending in either New York or Bronx County or other counties in New York City—those cases were dismissed. Some of them had still been pending. The New York City courts are not notoriously caught up in the Criminal Section with people awaiting trial. And in some of the pending cases, which I don't think I am at liberty to give the names of, those cases were dismissed.

Some of them, I might point out, were not cases where the people had any money taken or had evidence planted on them. In fact, in some of those cases, it might be fairly argued that the evidence which would result in their convictions could be characterized as not the result of the illegal wiretapping or bugging but the local prosecutors in the interest of justice, given the witnesses who would have to testify and given their reputations which, as a result of our investigations, were more than seriously scarred as to credibility—they decided to dismiss those cases.

MR. HERSHMAN: We have also been told that perhaps as many as 200 narcotics cases at this point are in question due to the possibility that evidence was obtained illegally. Would you comment on that?

MR. JAFFE: I can't give you the numbers. I can tell you that where we have gathered evidence and have not been able to file federal indictments, the evidence has been turned over to the Special State Prosecutor in New York City. And if there is any evidence that the cases that they come out of are cases where the defendants were indicted or convicted based on the illegal evidence, steps are being taken to be sure those convictions or pending cases are dismissed if that is warranted or that the indictments be dismissed and the sentences removed. I can't give you an idea of the number.

MR. HERSHMAN: Mr. Jaffe, you also state there might have been complicity on the part of the

Assistant District Attorneys of the City of New York. Have there been indictments or prosecutions of these Attorneys?

MR. JAFFE: There have not in our district been indictments. Whether or not there will be, I am not at liberty to say. I can only say the matter is pending investigation.

And perhaps it would be a good point here to interject something I would have liked to have interjected when one of your other witnesses was testifying.

You cannot investigate official corruption cases quickly, whether you are an assistant with seven other assistants and a very limited office investigative staff to help you, or whether you are the state prosecutor who has a tremendously large staff to help you. The types of cases we do cannot, for the most part, be done overnight. They can be, when you get a person who could be a defendant and he decides to cooperate and you thereafter corroborate what he says. But if that is not the case, and even when it is the case but the person has serious credibility problems, you have to be able to spend the time to develop the cases.

Sometimes that can be done in a month. Sometimes it takes three years. But the fact that there have not been indictments, for example, in the cases that we investigated and some of which have been turned over to the Special State Prosecutor for prosecution—and by that I mean the Special State Prosecutor for the criminal justice system in New York City—the fact it takes time doesn't mean that the job doesn't get done. In these cases, when these witnesses are scarred because their criminal involvement has been so total in certain areas, you have to be able to develop your case carefully so when you get to a jury and you try the case, you win it.

You cannot indict public officials in the hopes that somebody will come up in the future to win your case. It is irresponsible because once they are indicted their public career ends. So you have to take time to thoroughly investigate the case. And as I say, the fact we have not had some indictments on matters that are public knowledge does not mean that indictments will not eventually be forthcoming.

MR. HERSHMAN: Earlier, one of our witnesses testified that it might be advisable to include a misdemeanor statute in the current laws. Would you comment on that?

MR. JAFFE: I don't think that the misdemeanor provision is necessary in this area. And I say that for this reason: There is a present misdemeanor provision which can be read to incorporate illegal electronic surveillance. That is a part of the Civil Rights Act. And the civil rights misdemeanor can

be read to incorporate illegal wiretapping. As a matter of fact, we have such a case pending in our court now which I cannot comment on. And misdemeanors are available through that section to incorporate the violations which also are included in the wiretapping section under Title III.

MR. HERSHMAN: Mr. Jaffe, the United States Attorney's Office in the Southern District of New York is somewhat unique. It is one of the two U. S. Attorneys' offices in the country that has independent investigative help. I believe you have criminal investigators assigned to your office. Is that correct, sir?

MR. JAFFE: That is correct. I don't know if we are the only two. It may be three or four. But it is a very limited number, and we have three criminal investigators assigned. One is here today. That is Mr. Bogen.

MR. HERSHMAN: Would you tell us to what use you have put these criminal investigators and how much they have aided your office in corruption cases, police corruption or otherwise?

MR. JAFFE: If we had five more like Mr. Bogen, we wouldn't need anybody else.

MR. HERSHMAN: I might add that Mr. Bogen is my mentor and has taught me everything I know.

MR. JAFFE: He has done a good job.

The criminal investigators we have investigate almost every branch of criminal law we have under investigation. They fill in gaps in certain areas for some agencies, for example—without naming specific agencies—and whether or not an agent will do certain types of investigations often depends on the manpower needs of that agency. It is a thing that I alluded to in my statement, and that is this: You need manpower and you set priorities on what you investigate. And as I believe the Chairman pointed out, if you don't like the priorities an agency sets, you try to change them yourself.

Now, we have been able to do that through people like Mr. Bogen and other investigators, because if we feel a matter needs special work we put our own investigator on that matter. And it gives us a form of help without which I think we wouldn't make the cases we make.

We are more fortunate, in addition to having Mr. Bogen and the other investigators, in having a very good cooperative effort with the police department of the City of New York. While it is true that you cannot as a rule investigate your own, New York City has a police department and a police commissioner, at least since the Knapp Commission era when the scandals broke, of which I guess Bill Phillips was a part, along with others—the police department has an Internal Affairs Division. It has field associates which are spread out all through the

police department. But in addition to that, they have a First Deputy Commissioner's Special Force.

Now, until the recent budget cuts, that was some 50 people. They worked liaison with federal agencies and they will investigate, as our own investigators do also, matters which other agencies will not go near. Agencies may not want to touch a case for a number of reasons, but when you have that type of manpower, plus, for example, the Drug Enforcement Administration in New York City has a special corruption group that they have work with us.

Until the IRS changed its policy and tried to draw all the agents back in for reasons best known to Commissioner Alexander, we had a group of special agents in Intelligence who would work corruption cases with us. That still goes on to some extent.

When you have that kind of manpower, or even with that kind of manpower, you still are understaffed. You don't have the equipment you need. You don't have the manpower you need. You don't have the money you need. And it is only if you give that kind of manpower and money to a United States Attorney or to anybody else in law enforcement that you are going to effectively enforce any law.

But more specifically with wiretapping, unless you have investigators who are free to act, who will work closely with the investigating or prosecuting attorney, whether he is state or whether he is federal, you are just not going to make your cases.

The statutory problem is not the problem. Interpretation is not really the problem. The problem is detection and how you can detect crimes depends on what manpower you want to assign to work those areas.

Now, it is inevitable if you conduct an investigation of the narcotics unit because they are stealing money and selling narcotics, that you come up with information that they are also illegally wiretapping.

That is not to naively assume that the only illegal wiretapping in New York City or anyplace else in the country is in narcotics. Wiretapping is a way of life, as we have been led to believe, with a lot of police departments, in a lot of different areas.

You cannot expect a person to come forward and voluntarily give up the information about his fellow officers. That just hasn't been the case in our prosecutions or in our investigations.

People come forward and give information for the most part when they are scared, when they are sure they are going to be caught and prosecuted, when they are already caught, or when they have a grudge.

Now, in order to get people to give up that information, we, and every other United States Attorney's office, need more manpower.

Congress just last week slashed the budget so there is no money for additional investigators this year. They also cut out 112 positions, I am told, for new assistants.

Now, if the country, or the Commission or the Congress wants us to investigate and wants us to prosecute and curtail the type of illegal activity that you ladies and gentlemen have been investigating for quite sometime, they have to give us the money to do it. And that is the thing we need the most.

MR. HERSHMAN: Is it a problem of money or of Justice Department policy that you can't get any more independent investigators?

MR. JAFFE: I don't know what the policy is now with regard to Justice saying we can or we can't.

I have been told—and I don't know whether this is official or not—that there are to be no additional investigators at this time. Now, whether that is the policy or not, I don't know.

I do know that our investigators have made a tremendous number of cases. They have done thorough investigations. They have worked closely with grand juries and with assistants so that the information we need to discover crimes and prosecute cases is there.

MR. HERSHMAN: Do you find reluctance on the part of the FBI to accept your investigators and to work with them?

MR. JAFFE: I think that that is changing. Because I think the FBI's policy on what kind of crimes they investigate is also changing.

I think the FBI is taking a much greater interest now in white collar crimes as opposed to crimes of violence, if I can characterize it that way.

I think that the Bureau, when they look into the corruption area, for example, or into white collar areas where you need a lot of financial help, people who are financial investigators—when that happens and they see the results we have achieved, I think they are much more prone today than they were perhaps two years ago to work closely with our investigators instead of the way the situation used to be.

MR. HERSHMAN: Do you know, Mr. Jaffe, why it is that only a few U.S. Attorneys' offices have the available services of independent investigators?

MR. JAFFE: I really don't know the answer to that. I don't know whether that is a policy decision made by Justice in a vacuum or a policy decision made by Justice in accord with other agencies.

MR. HERSHMAN: Mr. Jaffe, in New York have these allegations of illegal wiretapping and these convictions of police officers interfered with legitimate police functions in court-authorized wiretapping?

MR. JAFFE: I don't think so. I think any time any agency, federal or state, conducts a legal wiretap, you have to be very careful and overly cautious. And the reason is this:

If you have a court-ordered wiretap based on valid, reliable information, an affidavit is prepared stating the probable cause. And the state and federal rules now in New York are very similar. Thereafter a judge signs an order for a certain number of days.

You must minimize, as I am sure all of you are aware. As you conduct your wiretap, if it is determined in the end that the assistant or chief assistant, or whoever it was that ultimately approved—and actually, with the Federal Government wiretap applications, go right down to Washington and then go back up. But if along the way the affidavit has been approved and the judge, relying on the affidavit, signs the wiretap order, and thereafter, with hindsight, two years later, the District Court or state court hearing the case says there was no probable cause, all your information is illegally obtained within the purview of the Fourth Amendment, you wind up with no case. Thereafter what you have to prove is that what you do have is not tainted. You also have to assure that your agents who were doing the planning of the wiretap are minimizing.

Now, if you are in the narcotics detection business, for example, if people talk about shirts and sheets and chess games, which they have in various cases prosecuted in our office, that is narcotics information, because how many shirts meant how many kilos, and the chess game meant, "I am going to make a delivery." But you have to be able to prove that, and you have to be able to justify listening the amount of time that you listen and making sure that you curtail listening to certain conversations.

And all of that presents a tremendous burden on the case. That is there, notwithstanding the fact of the illegality.

The problem that I think has been created is with the number of officers involved in narcotics detection under suspicion, arrest, or conviction, the number of police officers who come into court and say, "I swear I had a confidential informant," is really doubtful at times. And I think the prosecutions we have had or the investigations we have had may have cast a lot of doubt on police officers' credibility. But that is a price you have to pay.

If you have a tryable case, you can try it and win it. If you win it and win it legitimately, fine. If you lose it, for the most part you will get your man again. And if you don't, then you don't.

But you cannot excuse the illegal conduct in order to say, "I have gotten a bad man and I have convicted him."

MR. HERSHMAN: Mr. Jaffe, thank you.

CHAIRMAN ERICKSON: Mr. Hershman, well done.

Chief Andersen.

MR. ANDERSEN: I have just one question.

With regard to the illegal wiretapping in New York State, prior to Title III, in '68 would this have been legal?

MR. JAFFE: I don't think so. I think under 605 of the Communications Act it still would have been illegal, at least the part involved with telephone wiretap.

MR. ANDERSEN: And the disclosure—

MR. JAFFE: No, the disclosure of that, I believe, would have still been a 605 violation. I believe under the state law it was illegal back then also.

MR. ANDERSEN: I am wondering if all this started with Title III passage or had it been a practice of investigation that then blossomed out in '69 and '70. Was there a background of this type of investigation prior to Title III?

MR. JAFFE: I can't say that there has been testimony about it, but I can say that some of the evidence we have indicates that it was not a new practice to illegally wiretap and illegally electronically surveil, that is, to bug people before the passage of Title III. I think it was a practice in certain areas.

MR. ANDERSEN: What you are saying is backing up exactly what you said in your statement, that once the illegal acts started, the rest followed suit and came to full bloom.

MR. JAFFE: That is right. And I think, Chief, one of the reasons for the blossoming, in part, was there was a major influx of narcotics in those years, that is, the years '68, '69, '70 and '71, and also a change in the set-up of the police department to form the SIU who were going to be people to do major investigations.

And when the determination was made to do major investigations, which used a lot of purportedly legal wiretapping—there was an awful lot of wiretapping done which was legal, and a good part of it is still apparently legal. But I think the opportunity presented itself, with the influx of a large number of narcotics dealers, having a unit set up to prosecute them or investigate them, and given the nature of the way the police department allowed the investigations to go on just made the opportunity.

So in those particular years—for example, in 1970 for one man was a boom year. We indicted him for it but couldn't prosecute him on it because

he was only extradited for selling narcotics. That is Peter Daley. In one year he was charged with \$137,000 income tax evasion. And he was not alone. Egan was charged for '68, '69, '70 and '71, and I believe it was in excess of \$40,000 or \$50,000 per year. But I am not exactly sure of it.

It was an opportunity presented due to the situation on the streets of New York.

MR. ANDERSEN: Thank you. I have no more questions.

CHAIRMAN ERICKSON: Thank you very much, Chief.

Judge Shientag.

MS. SHIENTAG: Thank you, Mr. Chairman.

You said in order to acquire the equipment, the detectives had to lay out their own money, and therefore felt justified in the beginning in helping themselves to the funds. You indicated that.

MR. JAFFE: Yes, ma'am. Let me explain it, if I could.

MS. SHIENTAG: I think I understand. But the point I am trying to make is that once the equipment was used, they could use the same equipment against other potential offenders.

MR. JAFFE: What they offered as the justification for their act was the payment for equipment.

MS. SHIENTAG: But in any event, it wasn't a good justification because this equipment which they acquired from surreptitious sources, not recognized sources, was not used exclusively and then thrown away, but was used again and again.

MR. JAFFE: No, that is not necessarily true. I think once the situation was established where they knew they could get the money, they would not necessarily care what they did with the equipment. They did reuse some of it, that's true, but a lot of the bugging devices they used for automobiles they'd lose and not try to recoup. There was one case which demonstrates it also. They had a receptacle device similar to the device demonstrated here today, except it fit within the wall. However, there was no room in the wall, because it was a plaster wall, to put the wire in, and it was left out and discovered. Thereafter, the police officers had no choice except to arrest the people, which they did, and I think stole \$35,000 from them.

It is no justification because other cases we have indicate that the SIU officers before '69 would routinely shake down their informants and steal money.

But for the people who came into SIU in '69 and '70, some of the justification they offered to juries and to us for stealing the money was, "We had to pay for the investigation anyway, and besides if we turned it in and vouchered it the way we should have, it only would have been given back and they would have kept it."

I don't know if that answers your question.

MS. SHIENTAG: Yes. I was only minimizing, to say that, the amount of money they spent—

MR. JAFFE: You are absolutely right. The justification is not there.

MS. SHIENTAG: With regard to the defendants whose rights were infringed by the police using illegal wiretaps, have any of them brought suit for civil damages?

MR. JAFFE: I don't know of any who have brought suit for civil damages. I know one or two were very happy to get out of jail and out of the United States. They weren't interested in recouping. They just wanted to leave.

MS. SHIENTAG: What about the case of Edmund Rosner, the lawyer?

MR. JAFFE: Mr. Rosner was not involved—there was no illegal wiretapping involved in the case on Mr. Rosner. Mr. Rosner was involved with paying a turned New York City cop named Robert Leuci. Rosner offered and did pay Leuci quite a bit of money in order to have Leuci get 3500 material, that is, material we have to turn over, for example, grand jury testimony, out of the Office of the United States Attorney of the Southern District of New York in a case in which Rosner was the target. Rosner was tried and convicted and there was an appeal which was affirmed.

I don't know whether the second appeal has been affirmed yet.

But thereafter, Leuci disclosed a lot of additional information to myself and other Assistant U. S. Attorneys. That was turned over to defense counsel. There was a subsequent hearing held. There was an appeal. I think that appeal was affirmed again.

Rosner's case was based on recorded conversations, I believe on Nagra recording equipment.

In fact, it was affirmed, because I think Judge Gurfur wrote the second affirming opinion, emphasizing that Rosner was convicted on the parts of Leuci's testimony which were corroborated by tape recorded testimony. That was one-party consent.

MS. SHIENTAG: That was consensual wiretapping outside of Title III?

MR. JAFFE: Yes, ma'am.

MS. SHIENTAG: Which brings me to this: You indicated Section 2511, subsection (d), permitting consent interception is one of the loopholes. Would you explain what you mean by that?

MR. JAFFE: Yes, ma'am. My reading—and I don't claim to be a definitive statute reader, but my reading of Title III, specifically those sections, is that, unlike other witnesses who have viewed it as a Swiss cheese full of holes, the statute says if you have knowledge of interstate shipment of parts or

the components or the device itself and you use it, it is illegal. And it seems that the only authorizing section, other than the sections that say that law enforcement or telephone communications people are excepted, is the section you just referred to.

And it seems to me that under the guise of one-party consent, that is, one party saying, "I am free to do this," the industrial espionage goes on because supposedly it is done with the consent of a party.

It seems to me that is the way the ads that still run in the *Times* and—

MS. SHIENTAG: The *Law Journal*.

MR. JAFFE: Or the ads that say, "Listening as a home baby sitter"—all that is consensual, and you are allowed to do it. And I think if you'd eliminate that type of loophole or tighten up on the manufacturers—and that probably doesn't refer to big companies who will be careful. It means taking the people who exist as your investigators know they exist, and instead of allowing them to sell on a pretense of, "I sell to police officers who show me a badge," maybe eliminating them and centrally registering all the electronic equipment that is available or absolutely prohibiting the manufacture except through certain channels.

And I know it may not be a good analogy. It is kind of like the manufacture of barbiturates and amphetamines which are manufactured and sold throughout the U. S. by prescription.

I can't imagine, and I don't think any Commission member can, that the number of pills manufactured is equivalent to what is consumed, and yet those companies are allowed to produce and produce. If they could tighten up on the production and perhaps if we could control the production of the eavesdropping devices in that way, that would be one way to control it.

But I think the statutory loophole is the part that says consenting conversations can be monitored.

MS. SHIENTAG: Thank you very much.

CHAIRMAN ERICKSON: Professor Blakey.

MR. BLAKEY: Mr. Jaffe, do you think that as a result of these prosecutions there has been a change in attitude in some of the agencies of the police department?

MR. JAFFE: I think so, to a limited extent. I think the change in attitude began when all the public pressure was focused on the police department—and perhaps somewhat wrongfully—with an assumption after the Knapp Commission report that every police officer in New York, at least, was on the take or was crooked.

That is not proper English, but that is the attitude that existed on the streets of New York. And I don't think that is fair.

MR. BLAKEY: There are a number of places in Title III that, frankly, presuppose a certain amount of trust on the part of society in their officers. In rules like minimization, for example, you have to take a lot of salt to believe the officer turns it off and on when he is supposed to.

But the kind of horror story you have told this afternoon, in a very forceful and dramatic way, is the kind of horror story that might cause someone who is sensitive about privacy considerations to say, "We might gain something in law enforcement by wiretapping, but there aren't enough good guys to trust the staff to do the work right. Maybe we can't afford to have the power around for the bad guys to abuse?"

I wonder if that is a fair conclusion to draw from what you have told us.

MR. JAFFE: I don't think so. It goes to what I started to say before. In any police department, in any commission, in any district attorney's office, any United States Attorney's office, in the Senate, in the Congress, in the judiciary, there are so many people who are trustworthy and a certain percentage who are not. The SIU are at the most 100 out of—

MR. BLAKEY: Just—

MR. JAFFE: Let me finish.

MR. BLAKEY: You can go back. You said there were 70 or 80 people.

MR. JAFFE: That's correct.

MR. BLAKEY: But the unit wasn't formed by an attempt to gather, in the 70 or 80, the most corrupt people in the Department. It was an effort to gather the most elite group.

MR. JAFFE: Yes.

MR. BLAKEY: Are you suggesting the 70 people were not representative?

MR. JAFFE: No.

MR. BLAKEY: I take it, to the contrary, that if you had two people in SIU or three people in SIU who weren't doing it and you had 68 who were, and they were typical of the whole department—and there is no indication for us to believe they weren't typical—you have said a great deal about the 30,000, and you have said a great deal about whether we ought to trust the New York City Police Department with this wiretapping ability.

MR. JAFFE: I wouldn't draw the conclusion you did for this reason: If you look at the structure of the SIU, it was, for the most part, unregulated. There was no top supervision. There was no top reporting requirement. The people in the group were allowed to function more or less as they pleased because the public wanted major narcotics dealers put away.

Since the time of that group, for example, we had a group of 86 people prosecuted by our office jointly with the New York State people, and the New York City people. The people controlling the officers, the people setting the atmosphere, the attitudes are much different.

MR. BLAKEY: Do you have any hope that it won't be the same? If we go back into history, we have Knapp now, but 20 years ago there was a Brooklyn grand jury, and 20 years before that there was a Seabury investigation. This goes back and back and back, and the next thing you know it's Teddy Roosevelt who becomes head of the police department in New York City in an anti-corruption drive.

MR. JAFFE: But that is true in every phase of life.

MR. BLAKEY: What bothers me about that history is that every 20 years or so we have had new corruption develop and be exposed—or is it that every 20 years or so we have had a look at what has been there all along?

MR. JAFFE: I think that is the difference with what we have now. We now have groups of people in special offices who are set up to do nothing but monitor the police themselves.

MR. BLAKEY: Do you think that is going to be successful?

MR. JAFFE: I think it has been successful. I think there is a considerable difference in what is going on. I won't say there is nothing like what there was going on now going on.

MR. BLAKEY: Substantially curtailed.

MR. JAFFE: Yes.

MR. BLAKEY: Let me ask you the first question last. Of all the people appearing before us, you are the first who has had his hands burned, as it were, with bad surveillance. It has not been a theoretical problem with you but a real one.

Would you now, given the opportunity to vote—would you vote to continue the wiretapping authority, the electronic surveillance authority, to the New York City police?

MR. JAFFE: Yes, sir, I would. I would do it, and I would do it for more than one reason.

The first thought is this: If you curtail it absolutely, it will go on regardless of the curtailment. And the best proof of that is what happened in Texas.

MR. BLAKEY: But I put that to the Chief of Police and I said: "Do you think if they had had a legal way of doing it they would have done it the legal way and not the illegal way?" And he said, "Yes."

MR. JAFFE: I say the answer is no, and I will explain the answer this way.

If you have a district attorney or a federal prosecutor who on every case with every person he works with says, "You do it the right way. You do it by the book. You do it constitutionally and legally. And if you don't, you will not only be dismissed; you will be indicted," that's a lot different attitude than saying, "Let's get this guy; I don't care how." And I think there has been that change in attitude.

I am not saying it is perfect, and I am not saying it will ever be perfect. But I think if you change the attitude of the people who prosecute and change the attitude of the police department—which has been changed considerably, maybe not because everybody is a good guy now but maybe because in every precinct there are five or six field associates who write down everything that happens and turn it in to the central office.

However it has occurred, though, there has been a substantial change. And I think the change can be best demonstrated by a person who was indicted in our court. His name is Gabriel Stefani. Stefani was a sergeant in SIU at the time most of this corruption went on. Stefani was a person who shared in monies, who did not share in narcotics, and as far as we have been able to determine did not participate in illegal surveillances. He wasn't totally trusted by the people he supervised. They would always not talk to Stefani. They would go to Egan who was the commander.

Stefani left SIU in 1970, I think it was, or '71. Nothing had been discovered about the illegalities that we later found out. Stefani had left. He was promoted to lieutenant.

Against his desire to do so, about six months later he was sent back to supervise this 86th investigation, as it was called. He did a job—and that was a case where we had two assistants from our office and an assistant from other offices supervising every phase of it.

Stefani was absolutely honest and absolutely by the book. The fact a person had been corrupt before doesn't mean he can't change. And I think the fact that more than a third of the then-existing SIU has been indicted and convicted and sent to jail has a substantial effect on all the police officers in the New York City area—maybe, indeed, throughout the country. I think there is that change.

And as to your hard question: Would I trust them again? I wouldn't trust everybody but I would trust a considerable number. And I would not get rid of the wiretapping or eavesdropping laws because I could conclude there was nobody I could trust.

I'd always be wary and watch everybody, but I do that by nature now anyway.

MR. BLAKEY: Thank you.

MS. SHIENTAG: May I ask one more question?

MR. JAFFE: Yes.

MS. SHIENTAG: With regard to these cases before Special Prosecutor Nadjari, did those cases arise in the Bronx or in Frank Hogan's office?

MR. JAFFE: You mean with regard to the police officers involved?

MS. SHIENTAG: Yes, the police officers.

MR. JAFFE: The police officers involved—SIU operated throughout the five counties. There was no restriction.

MS. SHIENTAG: So the District Attorneys—you said in your prepared statement that certain District Attorneys blinked their eyes at what was going on; were those District Attorneys in Manhattan or the Bronx?

MR. JAFFE: First, I wouldn't say where they are because it is still a pending investigation. But I would not conclude they were just limited to the two boroughs of Manhattan which are in our district.

MS. SHIENTAG: There is only one in your district?

MR. JAFFE: No, Manhattan and the Bronx are in our district, but the officers also worked in the three other boroughs in New York City. And where those District Attorneys worked—I wouldn't conclude they happened to be either in the Manhattan or Bronx DA's office. It may be another, but I am not at liberty to discuss it because it is still a pending case.

MS. SHIENTAG: The only reason I ask is because we have heard so much testimony about Frank Hogan's office being so honorable.

MR. JAFFE: I would really like to but I can't comment on that.

CHAIRMAN ERICKSON: I just have a few questions, Mr. Jaffe, and I might say the information you have provided us has really fleshed out the reports in some areas where we needed testimony just such as yours.

Can you tell us whether or not you used the FBI to investigate these illegal taps that were being conducted by the New York police?

MR. JAFFE: No, sir, we did not.

CHAIRMAN ERICKSON: Can you tell us why you did not?

MR. JAFFE: There are a number of reasons.

The first is the investigations primarily involved activity in the narcotics area. The activity in the narcotics area we made a determination ought to be investigated by the Drug Enforcement Administration, the DEA, for among other reasons we had a special corruption group from them assigned to us.

We also determined that since there was a lot of police personnel involved, we could use the people from the First Deputy Commissioner's Special

Force to aid us in securing all the police records and other materials necessary.

We also used the Internal Revenue Service once it was determined that we would have sufficient monies to be found where financial investigators would be important.

More importantly, aside from the wiretap violations which we really didn't have pinned down at the beginning of the investigation, the only other statutory authority other than narcotics we had was obstruction of justice. And since it was obstruction of cases involving the narcotics enforcement, I believe that part of the policy—and I don't know that we even asked the Bureau into that investigation, but I think part of the policy is on obstruction cases, while they have jurisdiction over obstruction, if it is within a matter that another agency initially had, the other agency should investigate it. But we had already established a very close liaison with three agencies, and we had a tight-knit group of people who would work very closely with us.

CHAIRMAN ERICKSON: Do you feel the complaint they made about Houston is well-founded, that it is difficult for the FBI to investigate and prosecute, if you will, the very police that they are cooperating with in other cases?

MR. JAFFE: No, sir, I disagree with that allegation. I anticipated that was a question, and I covered that in my opening statement. If we are to conclude that any federal agency—any, not just the Bureau—cannot effectively investigate local law enforcement, then we are going to have to take the view that we ought to do away with cooperation among agencies, that is, local and federal.

I have never seen any evidence that the FBI or any other federal agency cannot effectively investigate local law enforcement corruption.

Now, it may be that if you have a small resident agency where one resident agent works on a day-to-day basis with one or two resident local police officers, or, in fact, a whole police force, he may not be the man to do it.

But to come to a conclusion that because the Bureau works with locals, therefore they cannot investigate the locals—I disagree with it completely.

CHAIRMAN ERICKSON: Do you feel it would be beneficial to bring in agents from another city to investigate a local police unit?

MR. JAFFE: It depends. And the reason I say it depends is not to hedge on the question, but there are times you need the resident agent to tell you all he knows. You may not want him to feed it back and you might want to bring in other people.

CHAIRMAN ERICKSON: It depends on the exigencies of the situation.

MR. JAFFE: That's it, Mr. Chairman. You cannot make a global decision.

CHAIRMAN ERICKSON: It is a matter of judgment.

MR. JAFFE: Yes.

CHAIRMAN ERICKSON: Have any charges been brought by reason of the investigation of the New York police under Title III?

MR. JAFFE: Yes, sir. We have a number of indictments. There is a case scheduled for trial September 3 or September 11—and I don't want to name the case.

CHAIRMAN ERICKSON: I'd prefer that you didn't.

MR. JAFFE: That case indicates there is a misdemeanor available because there are people within the case charged with civil rights misdemeanors. That case is not exclusively a wiretapping case because the allegations include the theft of, I think, \$7,000 or \$8,000 from the narcotics offenders who were relieved of that money by the officers. The way they relieved them of the money was through an illegal wiretap and an illegal bug.

One other thing you might want to consider, Mr. Chairman. In prosecuting cases solely on accomplice testimony which we often do, where a co-conspirator or another person involved with the person decides to cooperate, there is more jury appeal if the case also involves taking money or violating a person's civil rights. And if you can combine the wiretapping case with that—here I am talking about corrupt police officers or law enforcement officials—it makes them much more triable cases.

With regard to other types of wiretapping cases—and there are current investigations in our office—those for the most part are cases that developed through our investigators or people who came in and were thereafter referred to the Bureau. Those are triable types of wiretap cases because the person who was the target of the wiretapping was almost like the victim of an extortion, and you can try that case because the people who were doing the extorting have the motive you can demonstrate to the jury, and therefore show their evil activity with regard to the wiretapping.

CHAIRMAN ERICKSON: Your office has cooperated with the New York police in some of these investigations?

MR. JAFFE: Yes, sir, that is so.

CHAIRMAN ERICKSON: And they have been helpful to you?

MR. JAFFE: I would say that we have made a considerable number of cases using the First Deputy Commissioner's Special Force. It may have been we would have preferred to use our own investigators or other agencies, but they were not available and they have made cases for us. And I will give you an example, although it is not wiretap related.

We have indicted and convicted the man who was second in command at the Selective Service Office in New York. His name is Sam Germino. And that case was made by the New York City Police Department and our office by the use of an investigative grand jury.

So the New York Police Department, so far as I have known it, has given us help in every conceivable area, so long as it is within their jurisdictional grounds.

CHAIRMAN ERICKSON: Mr. Jaffe, I thank you. I appreciate your coming here and I want to say your office and investigators have been most helpful, and they have pointed out why this probable cause reference enunciated in the Fourth Amendment, enunciated in *Katz* and *Berger*, are such a key part to the right of privacy, and why the protection of that right is totally consistent with law enforcement.

Thank you very much for coming.

MR. ANDERSEN: Mr. Chairman, could I have 30 more seconds?

Mr. Jaffe, have you done any investigating of federal agents in the same area?

MR. JAFFE: Yes, sir.

MR. ANDERSEN: Is that under your jurisdiction?

MR. JAFFE: Yes.

MR. ANDERSEN: Do you feel that is one of your responsibilities?

MR. JAFFE: It is most assuredly.

MR. ANDERSON: I am comparing it to the Houston case. Do you feel the policing of the FBI in those cases is the district attorney's responsibility?

MR. JAFFE: If I may, Chief, I'd like to break it up, if I could. We routinely, together with, for example, the IRS Inspection Service, have indicted and convicted bad Treasury Department personnel for bribe-giving and receiving, for obstructing justice, for taking money, for selling out investigations. Together with DEA Inspection, we have investigated and convicted narcotics agents for doing the same thing. It is our responsibility to do that because they are federal employees.

With regard to state employees—and let me just finish the thought on the first section first.

If there is evidence that federal agents did the same acts that state agents did, that is, that the SIU did, they stand in no better or no worse stead. If they are guilty of a crime and we can prove that they are guilty of a crime—whether or not we can, we are going to completely investigate it and try to arrive at a conclusion, and if the man should be prosecuted he will be.

With regard to the police officials in the City of New York, New York City, unlike most cities but like—for example, Philadelphia now has, and I think other cities are establishing the office of a Special Prosecutor for the criminal justice system . . .

[Off the record.]

I was saying that he is primarily charged with looking at the criminal justice system. That doesn't mean that we don't look at it also. And the reason is because if there are state violations that police officers are involved in, and given the cooperation that exists between state and federal and local agencies, it may very well be that our investigation will lead us back to people that we ought to be primarily looking at. So it is a shared responsibility.

Now, one of the reasons we turned as many cases over as we did is because many cases may be better state law violations and better prosecuted in the state section.

There is an additional reason in New York. There is an act called the Hughes Act. That gives the prosecutor an extra five years statute of limitations. In New York State, the statute doesn't start to run until five years after a public official has resigned from public office. We don't have that.

We are limited.

MR. ANDERSEN: Thank you, Mr. Jaffe.

Nothing was said about that area of your responsibility—

MR. JAFFE: Our area includes all the federal agencies and their corruption, plus any public official.

MR. ANDERSEN: Thank you, Mr. Jaffe.

CHAIRMAN ERICKSON: Mr. Jaffe, we appreciate it very much, and we might say also thank you for the training which your chief investigator gave our Mike Hershman who distinguished himself today.

MR. JAFFE: Thank you, sir.

CHAIRMAN ERICKSON: We stand recessed until 9:30 tomorrow morning.

[Whereupon, at 5:30 p.m., the hearing was adjourned, to reconvene at 9:30 a.m., Thursday, June 26, 1975.]

[The following news account reports another example of suspected illegal wiretapping by police, but was brought to the attention of the Commission too late to be included as part of the hearings on illegal wiretapping which were conducted in June, 1975.]

September 8, 1975

FBI delayed its probe in Jeffco wiretapping

By JACK OLSEN JR

News Staff

Last spring the Denver office of the FBI waited nearly one month before investigating the criminal implications of an unauthorized wiretap placed by four Jefferson County sheriff's officers, one of whom had worked closely with the FBI and admitted the eavesdropping to an FBI agent.

Then the federal agents moved on the case only after being told to do so by U.S. Atty. James Treece on the same day Treece was told about the wiretap by his subordinates.

The four deputies, who included the captain of the sheriff's intelligence unit, Donald V. Edwards, subsequently were found to be unprosecutable because a statute of limitations required that charges have been filed within five years of the eavesdropping crime.

The wiretap allegedly was put on the phone line of a suspected gambler in Lakewood, Joseph Nicholas Raso, in the summer of 1970. Partly because of the FBI's delay and partly because of unclear or inaccurate communications between the FBI and the U.S. attorney's staff, the government didn't realize the statute of limitations was a serious factor until about 9 days after it was too late.

ACTION DELAYED

According to the FBI confidential file on the case, which was made available outside of official channels last week, the FBI didn't start investigating the wiretap with a view toward prosecuting the sheriff's deputies until 27 days after the bureau learned about it.

FBI special agent William J. Malone was informed of the tap — and that it was "unauthorized" — by Edwards on June 19 of this year. The federal agent realized the seriousness of the matter because he quickly suggested to Edwards, who is a widely respected law enforcement officer, that he not say anything more but contact a lawyer.

Illegal wiretapping is a felony that can bring a five-year prison sentence.

According to Assistant U.S. Attys. Thomas Alfrey and Daniel Smith, whose job it would

have been to make certain the case was filed in time, Malone told them that Edwards had confessed that the wiretap took place in December 1970, "possibly up through the Super Bowl (a professional football game in January)," Smith said.

But when Malone filed his report on the matter — about one month after Edwards' confession — he wrote that Edwards had admitted the wiretap was in the summer or early fall of 1970.

Had the federal prosecutors known the contents of Malone's written report, that the eavesdropping crime was earlier than December, they would have moved faster, possibly even calling a special session of the federal grand jury, they said.

The three other sheriff's deputies involved were Raymond Taylor, who like Edwards is still employed as a Jefferson County sheriff's deputy, and Kirk S. Steinmark and Ronald D. Ralston, who both now operate a bar on Lookout Mountain.

According to the U.S. attorney's staff, after Edwards' confession to Malone on June 19, the four wiretapping suspects refused to cooperate with the FBI or give any more details of the illegal wiretap until an Aug. 20 hearing in the U.S. District Court in Denver. Then Edwards testified that the tap had been removed Aug. 10, 1970 — five years and 10 days before.

It appeared then that the deputies had been saved by the statute of limitations and their own refusal to talk before Aug. 10, 1975. Last week, Raso's lawyer, James L. Gilbert of Arvada, filed a motion in federal court in which he suggested that the four deputies had been "less than truthful."

Prosecutor Alfrey later conceded that the government had been "outsmarted."

FEARED RUIN OF GAMBLING CASE

The FBI file on the case indicates that from June 19 until mid-July the dominant concern of the FBI and the prosecutors was whether the illegal wiretap was going to ruin a recent gambling case against Raso, whose apartment had been the target of the phone tap.

A federal judge ruled after the Aug. 20 hearing that any evidence gathered from the illegal 1970 wiretap wasn't used to build the recent case against Raso, who was arrested in May with six others on suspicion of gambling. Had there been such "tainted" evidence, Raso's case might have been thrown out of court immediately.

Raso's attorney, Gilbert, now contends that the wiretap was in use long after Aug. 10, 1970, possibly into 1971 and 1972 as well, and that the four deputies still might be prosecutable. And Gilbert contends that gambling discussions, rather than innocent conversations, had been overheard. Edwards denied it, saying the tap didn't help them in the investigation of Raso at that time.

(Edwards and his three fellow deputies destroyed all evidence of the wiretap, they said. There is no documentary evidence, therefore, to support or disprove their assertions as to the crucial date of the wiretap or the contents of conversations monitored.)

There is some evidence that Gilbert is right, that the illegal eavesdropping was more extensive. Gilbert claims a "source" has told him these additional details, which he has turned over to the U.S. attorney's staff. It is no ordinary source, the FBI has determined.

According to the FBI file, Wheat Ridge attorney Maurice Fox admitted he was the source who had told Gilbert about the wiretapping.

PRESSING FORWARD

"Fox said he did not care to divulge where he received this information," the FBI report says. The FBI pressed him on that point, with good reason. Fox is the defense lawyer for two of the wiretapping deputies, Steinmark and Ralston.

"He was getting his information from the horse's mouth," said an assistant U.S. attorney.

The FBI report said federal agents had pointed out to Fox that the information "had to come from either Steinmark or Ralston."

It seems possible that had Raso not been arrested in May for alleged gambling, this Pandora's box might never have been opened.

After Raso's arrest, Gilbert said he was contacted by his source — whom the FBI confirmed is Fox — and was told about illegal wiretapping not just in the summer of 1970 but into 1971 and possibly 1972. Gilbert is known to have been told the gist of some of Raso's phone conversations that were monitored — supposedly in December 1970 — and he is known to have checked them with Raso, his client. Raso allegedly recalled some of the conversations.

On June 18, according to the FBI report, Gilbert called Edwards into his office and told him he thought there was something suspicious about the way Raso had been investigated back in 1970.

Gilbert says he purposely didn't mention wiretapping, but Edwards did, denying that he'd ever done any illegal eavesdropping. (Edwards would later claim that Gilbert was ille-

gally or unethically applying pressure to get the gambling charges against Raso dropped. The FBI indeed investigated Gilbert for obstruction of justice and, according to the U.S. attorney's staff, cleared him of any wrongdoing.)

THEN ARRANGED MEETING NEXT DAY

While Edwards denied illegal wiretapping to Gilbert when Gilbert confronted him, the next day he arranged a meeting with FBI special agent Malone, a friend with whom he had worked sometimes closely in the previous five years. Inside a Wadsworth Avenue restaurant, according to the FBI report, their conversation related to Gilbert's allegedly improper conduct in applying pressure to authorities.

It wasn't until the sheriff's captain and the FBI agent walked to the parking lot, the FBI report says, that Edwards admitted the illegal wiretap. The report says: "Capt. Edwards advised that in 1970 either in the summer or early fall of that year" he and others "had conducted unauthorized wiretap . . . for approximately two or three weeks."

"Capt. Edwards was then advised," according to the FBI report, "that this matter could possibly involve some federal violations and, therefore, before he made any further statements he had better contact an attorney."

It was an unusual act by an FBI agent. Federal agents are to take a confession after advising the subject of his legal rights.

FBI agents also are to make prompt written reports of such confessions, or of any interview that likely will be used in a court case. The assistant FBI agent in charge of the Denver office, Simon Tulai, said last week that a U.S. Supreme Court decision requires that such reports be completed within five days of the conversation on which they are based, or they can't be used in court.

According to the FBI file, Malone didn't make his report on Edwards' confession until nearly one month later, on July 18, and then it was two days after the U.S. attorney told the FBI to start investigating the criminal culpability of the four deputies.

In the meantime, said Alfrey and Smith, Malone told them Edwards had confessed that the wiretapping was in December or later, not summer or "early fall" as Malone wrote in his report. The U.S. attorney's office didn't get the written report until late July, Alfrey said.

AWAIT MOTIONS

Malone didn't tell the U.S. attorney's staff about the illegal wiretap until one week after he learned about it. But the delay probably didn't have much effect, because there was little action by prosecutor Alfrey when he was informed.

According to the FBI report, "He (Alfrey) advised that before taking any further action in this matter, he could wait to see what motions were filed by defense attorneys."

Two weeks later Alfrey was still waiting for the defense motions. They were delayed, but Alfrey said there seemed to be no need to rush

anyway, because Gilbert had revealed more details from his source, including that the wiretap was in place in December — which Malone had reported verbally — and later.

"We knew we had four months at least before there would be a time problem (with the statute of limitations)," Alfrey said. "We had four months to take this before the grand jury," he said.

Looking back on it, Alfrey said, the delay was "inexcusable, and he readily took partial responsibility for it.

Malone presently isn't permitted to tell his side of the story. The FBI forbids its agents to comment about investigations or pending court actions. The agent in charge in Denver, Theodore Rosack, said little that was pertinent except that he believed there was a "misunderstanding" that had given the reporter an inaccurate view of the matter. He warned: "Make sure you have your facts right."

The FBI file shows that Alfrey on July 15 "was concerned over the possibility of some police officers being involved in an illegal wiretap.

"Mr. Alfrey," the FBI report said, "stated he was a close friend of the police officer whose name is Ray Taylor (one of the four sheriff's deputies involved), and that he would contact Taylor within the next day or two and get the full story from Taylor."

Alfrey did that, and Taylor either refused to be read his legal rights at the start of the conversation or once having been read them refused to discuss the wiretap.

Alfrey and fellow prosecutor Smith went to their boss, Treece, the same day, the FBI report shows.

"I got a letter out the same day," Treece said. It was hand-delivered to the FBI, and, Treece said, it instructed the bureau to start two investigations, one of the criminal wiretap and one of the impact of that tap upon any federal case.

"In a conversation with Alfrey," Treece added, "we kicked around the probability that the FBI had known about this for a long time. (We conjectured) what if Malone has known about this for five years. We seriously considered whether he should be a subject (of the investigation) too,"

They decided Malone need not be, but they asked the FBI not to assign any agents from the FBI organized crime unit in Denver to the case. Edwards had sometimes worked closely with members of that unit.

The FBI then conducted an extensive investigation in a few days, their file shows. By then, however, Edwards wasn't cooperating with authorities. He would say nothing until the prosecution deadline passed.

One page of the FBI final investigation report noted: "This investigation is predicated upon a letter dated July 16, 1975, from U.S. Atty. James L. Treece to Ronald L. Maley, (then) special agent in charge, FBI, Denver.

"Mr. Treece advised in this letter that it had come to his attention that in the fall months of 1970, the Jefferson County sheriff's office had an illegal wiretap. . . ."

It had come full circle. The FBI had learned of the crime on June 19. The U.S. attorney's office (Alfrey) had been informed by the FBI on June 26. The U.S. attorney re-informed the FBI on July 16 and gave the bureau's Denver office something upon which to "predicate" an investigation.

Treece, Alfrey and Smith apparently aren't going to let the matter die. It will be taken before the federal grand jury later this month, and then Gilbert likely will have to tell all that his source, Fox, told him about illegal wiretaps after the summer of 1970.

One of the four deputies, Steinmark, refused to testify in the Aug. 20 hearing, claiming that his statements might jeopardize him in a supposedly unrelated criminal case.

Sources in the U.S. attorney's office confirm that Steinmark will be granted immunity from prosecution before the grand jury and therefore won't be able to claim that his statements could incriminate him. He won't be able to remain silent.

Said Alfrey: "Steinmark will make us or break us."

Edwards explained that in the summer of 1970 he had gotten word that one of his street sources possibly was in danger from alleged mobsters the source was spying on. Edwards said he believed the only way to protect the source was to tap a telephone. And, he said, he knew the courts wouldn't give him permission to do it.

Subsequently a storeroom was broken into and the tap was installed on telephone lines passing through there. Weeks later, the wiretappers destroyed all the evidence of their wiretap, including tapes, Edwards said.

Hearing, Thursday, June 26, 1975

Washington, D.C.

The hearing was reconvened at 9:35 a.m., in Room 6202, Dirksen Building, William H. Erickson, Chairman, presiding. Commission members present: William H. Erickson, Chairman; Richard R. Andersen, G. Robert Blakey, Samuel R. Pierce, Florence P. Shientag.

Staff present: Kenneth J. Hodson, Esq., Executive Director; Michael Hershman, Esq.

PROCEEDINGS

CHAIRMAN ERICKSON: Ladies and gentlemen, may we convene this meeting.

This morning we are going to examine the rather difficult subject of illegal political wiretapping.

We are honored to have as our first witness Mr. Allen E. Ertel. Mr. Ertel is currently the District Attorney for Lycoming County, Pennsylvania. He is a partner in the firm of Ertel & Kieser. Mr. Ertel will discuss the investigation resulting in the 1974 conviction of Mayor Coder of Williamsport, Pennsylvania on charges of illegal wiretapping.

Mr. Ertel, will you come forward.

[Whereupon, Allen E. Ertel was duly sworn by the Chairman.]

CHAIRMAN ERICKSON: I believe you have an opening statement.

MR. ERTEL: Yes, gentlemen.

CHAIRMAN ERICKSON: You may proceed.

TESTIMONY OF ALLEN E. ERTEL, DISTRICT ATTORNEY, WILLIAMSPORT, PENNSYLVANIA

MR. ERTEL: I was asked to discuss four different topics by your Executive Director in his letter. One was the difficulties in prosecution; two, the difficulties of interpretation of both the federal and state law; three, the prosecution of Mayor Coder and his cohorts; and, fourth, the aggressiveness of the FBI and federal agencies in investigating the particular incident in Williamsport.

But before I do that, I would like to speak just briefly about the statutes and the competing policies that I have looked at behind these statutes and how they affected the prosecution in Williamsport.

Quite frankly, many of our statutes are under the rubric of right to privacy, but we don't know what policy we are effectuating by our statutes in what

was basically happening in the City of Williamsport and in other wiretapping situations with which I am familiar.

I think it is important we have these right to privacy statutes but they must also be offset against the public interest.

People want to speak freely and be able to exchange ideas without having Big Brother look over their shoulder and determine what they want to do in the privacy of their own particular relationships.

In the Williamsport situation we found that the idea behind the wiretapping, at least what we thought was the idea behind the wiretapping, was the obtaining of information for political purposes.

As many of you know, the obtaining of information, itself, becomes a power base from which one can operate, whether illegally or legally.

What happened in the City of Williamsport was there was wiretapping of the government agencies within the City Administration. It got to the point where police officers were reluctant to discuss pending prosecutions or pending investigations on the telephone because they suspected that their communications were being tapped, both in the City Hall on wire, and also the fact that even discussions within their own confines in their own police department were being listened in to by other individuals who were not privileged to listen.

So what happened is we had police officers who were afraid to discuss anything which pertained to their official position because they were afraid of exposure of that particular information prematurely or information that should not be disclosed at all.

On the other hand, we have the consideration that the police officers do need some sort of rights—or the government, or the public—to determine when there is illegitimate conversation. Most criminal activities have to have some sort of conversation to take place, whether it be a criminal conspiracy or anything else. And unless you have an ability to determine what is happening in those conversations, the police function or the public function sort of goes downhill in the prosecution of alleged criminals. And it is a balance between those two things that is necessary.

I have looked at both the federal and the state statutes. I understand Mr. Phillips did discuss the Pennsylvania state statutes with you yesterday, but

they are quite a bit different than the federal statutes which now exist under the Crime Control Act.

The Pennsylvania statute as it existed prior to the beginning of this year required that both parties consent to the interception or interference with any wire communication, or basically telephone or telegraph. In other words, both of us would have to agree that you could listen in, which was nonsense. What it meant was an absolute prohibition against anybody interfering with any phone conversations.

There is a case in the State of Pennsylvania—and it was one of the situations that arose in the Williamsport case—where a person recorded his own conversation with somebody else. Thus, if I call you, I want to record that conversation to protect my credibility. That could not be admissible in a Pennsylvania case. There is a Pennsylvania Supreme Court case in which a chap called up a fellow and said “I have a contract to kill you. I will reverse that contract and kill the person who hired me for an extra amount of money.” The person who received the phone call wanted to protect himself and prosecute that individual. He put onto his telephone a device to record that conversation. The Pennsylvania Supreme Court held it was inadmissible in the trial of the case and, as a consequence—I don’t know the final result of the case—but certainly it became the issue of credibility between one person and another.

CHAIRMAN ERICKSON: When was that case decided? Was it before or after the enunciation of the *Rathbun* case?

MR. ERTEL: Oh, much, much after *Rathbun*. It is quite an old case. *Rathbun* is the one-party consent which is under the federal law.

CHAIRMAN ERICKSON: *Rathbun* was an extortion case very similar to that where there was the overhearing on an extension phone, as you will remember.

MR. ERTEL: Yes, I do recall that case. But the Supreme Court case in Pennsylvania was within the last couple of years. I can’t give you the exact date. It was in the Seventies, and *Rathbun*, I believe, was in the Fifties.

CHAIRMAN ERICKSON: That is right.

MR. ERTEL: The Pennsylvania statute says specifically you need the consent of both parties. This was prior to the new particular statute which Pennsylvania has passed which was effective in February of this year.

Now, in February of this year Pennsylvania has passed a statute which defines eavesdropping. The Pennsylvania statute previously only went to interference with telephone and telegraph. Now you cannot overhear, listen, or record any other conver-

sation without consent of both parties. Again, it requires both parties’ consent. And therefore you cannot—if I were to send a drug informer, which is common, into a drug situation with a microphone on him and we would record the conversation, that is inadmissible in the State of Pennsylvania today, even though the one person party to the conversation agreed to it.

And in fact, not only is it inadmissible but the officer has committed a crime if he does it. It is a misdemeanor second degree in the State of Pennsylvania if you do that.

I might give you an example of a situation where this particular statute applied, where the federal statute would. As a result of the wiretapping cases in Williamsport, the political figures, the Mayor and a friend of his, determined that the way to stop the prosecutions of the city officials was to obtain evidence on myself as the prosecuting attorney and attempt to blackmail me into dropping the prosecutions.

As a result they contacted a young lady who was to do what is probably as old as time itself—was to obtain either someone else or herself and get me into a motel room with the appropriate photographer and pictures. And those were then to be used to blackmail me into dropping the prosecution of the existing Mayor and police chief in the City of Williamsport.

The girl, instead of doing as requested, went to the State Police and we then sent her back to determine her credibility, because her credibility was at stake. And we put a bug on her and we had, of course, undercover men in an appropriate vehicle with a receiver. And we recorded the conversations that took place.

Now, had that situation been tried without the particular microphone and the recordings, it would have been the question of her credibility versus the defendant in that case.

And I would suggest that there would not have been a conviction, because when you attempt to do something like this, the person you solicit to do it certainly isn’t a bishop that you are asking to do it and the credibility of that person would be at issue.

CHAIRMAN ERICKSON: It is something like the *Osborn* situation.

MR. ERTEL: That is right. But under Pennsylvania law today, as it exists, that is illegal—not only illegal, but it is criminal and inadmissible in a court of law.

So the Pennsylvania statute which really comes under the rubric of right to privacy, in my view really comes within the rubric of right to corrupt. There is no way to really have an effective prosecution of a bribe attempt of public officials; there is

no way to have a very good, iron-clad drug prosecution from an undercover informer. It is very difficult in a one-to-one situation, if you want to develop an iron-clad case without the means of electronic recording.

I think if this Commission is going to recommend any change in the federal law, certainly I would not use the Pennsylvania law as a model. I would suggest that is the exact opposite of what one would want to look at.

Turning briefly to the Williamsport wiretapping situation, I will give you a few of the details of the case and hopefully tell you some of the difficulties I encountered, and I think they are the same difficulties you would encounter in any prosecution like this.

I am familiar with prosecution of police officers in Mercer County, Pennsylvania where they were allegedly wiretapping people in the drug trade. Those prosecutions were unsuccessful. I happened to try the case of Mayor Coder in Mercer County because it was transferred in venue to Mercer County so I was familiar with the prosecutions that took place there.

In that particular case there were police officers allegedly wiretapping and there was no countervailing evidence at the trial, but yet the jury elected to find them not guilty even though the Commonwealth at least made out a prima facie case of wiretapping.

I think that points out one of the difficulties in the wiretapping situation. Many times when people are wiretapping and invading rights to privacy they are public officials or at least public employees. The public, I do not think, takes a very strong view against wiretapping. I think they feel that wiretapping is a legitimate function of government. I am talking about the general public; I am not talking about selected individuals within the public. And therefore, they will tend to find a person not guilty in a trial situation, especially if it is a government official.

What happens, and what happened in the Williamsport case was they try to get within the rubric that they are doing their duty, doing their job in doing the wiretapping. Whether or not it is political rather than part of their function or not, the defense normally comes up that it is part of their job. And therefore they jury sometimes accepts that. And that was the defense in the Williamsport case.

In the particular Williamsport case, I was contacted initially by counsel saying that his phone calls were being intercepted, that he had had a conversation with the Director of Public Finance in the City of Williamsport; he did not think anyone had

disclosed that conversation. But it had come back to him, the exact words he had used in that particular conversation.

I thought probably this was a political ploy and was not going to become involved. However, subsequently, I did agree to make one check for him to see if, in fact, such a thing existed. I called a police officer who allegedly had some information—and this shows you the paranoia of people who are involved in the wiretapping situation and of the police department at that time.

The first thing he told me on the telephone was "I won't talk to you on the telephone."

I have never had that point-blank statement from a police officer in my life.

I said, "Then I will come to your home and speak to you."

"Don't come to my home."

"Do you want to talk about the situation?"

We arranged then to meet in private. This person was so upset by the situation that existed that we met at my home and he at that time disclosed to me the tapping of telephones in the City Hall of the City of Williamsport in which he had participated.

He was a Corporal in the police department. The Captain was involved, the Director of Public Safety was involved, and the Mayor of Williamsport was involved.

I learned of the tapping of another police captain. That is all I learned at that particular point.

I later found out, in an entirely separate situation, there was a tapping of other people in the city, although not involving this police officer. So there was extensive tapping going on.

We know of about 50 to 60 phone calls approximately that were tapped. We do not know of the extent beyond that, although one can surmise from all the inferences that one picked up.

In any event, after having received that, and the difficulties you encounter especially when there are political figures involved, or public officials—normally in the State of Pennsylvania I do not have investigating staff attached to the District Attorney's Office. In the larger counties they do. We call on the State Police for assistance. In this particular instance I did call on the State Police for assistance. I was assured of assistance up through the Regional Commander, a Lieutenant Colonel in the State Police. I have always had the assistance of the State Police in any investigation.

I received a phone call later the same day from the Commissioner of the Pennsylvania State Police's office through the Captain of our barracks, advising me that they would no longer participate in the investigation, even though they were convinced there was a prima facie case and that the

sources and the information—I had this particular individual to speak to them. They were very chagrined by it but said they would not work on the case at all.

I then called the Commissioner's office directly and was assured of the same thing, and I then called the Governor's office. I advised the Governor that if I did not receive the cooperation of the Pennsylvania State Police and their investigative talents and abilities I would hold a press conference and explain that I had prima facie evidence of wiretapping in City Hall and that the Pennsylvania State Police refused to investigate.

Needless to say, that night I received the cooperation of the Pennsylvania State Police and no press conference was necessary.

As a result of that, the Pennsylvania State Police did investigate. I later learned that the FBI had been contacted by the Mayor of the City of Williamsport, the local office of the FBI, where they had discussed and he had brought to them a tape recording of a telephone conversation which allegedly had been made by a captain of the Williamsport City Police. This telephone conversation, recorded on tape, was played to the FBI with the allegation by the Mayor and the Director of Public Safety, who had taken it there, that their lives were in jeopardy.

According to later testimony by those agents, they thought it was strictly a political thing. The individual involved said, "We will get rid of them"—which meant politically—and they did nothing.

The matter of the way they told the FBI, according to their testimony, was that they had overheard it on the extension telephone and it had been an inadvertent overhearing of that particular conversation.

MR. HERSHMAN: If I may interrupt, they just happened to have a tape recorder there at the same time?

MR. ERTEL: That was my question. I said "How did you get the words 'hello' on the tape recorder if it was inadvertent? How did you attach the tape recorder to the extension phone which you had just picked up?" Obviously it didn't make sense.

But, in any event, the FBI advised the Mayor at that time to desist what he was doing.

CHAIRMAN ERICKSON: That is what they called inadvertent planned interception?

MR. ERTEL: I think that might be a good way of putting it. But at any rate they told them to desist and did not do anything further. And this was in June of 19—I forget the year now. I get mixed up in my years, it has been so long since this thing has been going on.

After that—this particular incident was disclosed to me by one of the officers in the FBI who, incidentally, was very cooperative. I spoke to him about it.

He also advised me that approximately eight months later they had a complaint to the FBI, after this tape recording had been presented to them. A complaint was made that City Hall was tapping phones. That was a unsubstantiated complaint, and later, through our investigation at least, we could provide no evidence of that particular individual's calls being tapped. But still the complaint was made. They had prior knowledge of this particular tape recording previously.

No investigation was done by the FBI at that time. This was three weeks approximately—I can't give you the exact date because it was never divulged to me—before we did the investigation that we conducted in the City of Williamsport.

So the FBI certainly had some knowledge or reason to believe that such things were happening in the City of Williamsport.

I disclosed to the FBI the extent of what I knew on the Saturday—Sunday morning I should say—prior to the convening of the special grand jury in Lycoming County. We attempted to convene that jury and there were motions by the defendants who had knowledge of what was going on to delay the special investigating grand jury and I don't believe it got started until the following Wednesday.

But in any event, we did do it and as a result we had a conviction of the Mayor of Williamsport after a two-week trial. The Director of Public Safety pled guilty after the primary case was in against him.

The individual officers involved were not prosecuted. They were government witnesses against the ones who were the perpetrators or the principal persons involved.

Turning to the difficulty in this particular matter, and most difficulties in both prosecutions of public officials and wiretapping, which overlap:

Number one, we could not obtain any physical evidence of the wiretapping itself. Once a wiretapper has any knowledge or when a conspirator breaks, usually they know and all evidence is destroyed. We never got any physical evidence in this case. We did get many statements, of course, which were just as good.

Secondly, unless you have one of these co-conspirators who turns around, very seldom can you ever get a prosecution in my view, because it is very difficult to obtain evidence. And especially if these people are in public life. Most of the people involved in this were responsible to the person involved and their jobs were on the line. And in fact

there have been repercussions to many of the individuals who testified in that case.

Secondly, we found that in the City Hall of Williamsport, even though it was prohibited by state statute to do any type of wiretapping because of the two-consent rule, there were wiretapping devices and strictly for wiretapping. They had no legitimate function. You could not convert those to a legitimate police function. These came to light some time after the investigation started. We could not prove conclusively they were used. There was a reasonable belief that they were but we could not prove it. It did come into the trial, however.

Unless you can get a co-conspirator to talk, you must have a stupid move by the co-conspirators or you can't find it out. In this case we did have such a stupid move.

The Mayor of Williamsport took one of the tapes and played it in the presence of the City Solicitor who did not report it, and also the Director of Public Services who was being talked about on one of these tapes by a City Councilman and the Director of Public Finance. His wife was also present at the time—it was somewhat of a party situation. There were six couples there.

The wife became extremely upset, realized what had happened, left the room, and went to a lawyer to determine whether or not she was criminally liable because she had overheard the conversation.

Subsequently, we had gotten information about this particular thing. We interviewed that woman. Quite voluntarily she came forward and disclosed what she had heard in that particular room. And this was another aspect of the wiretapping which we did not know about.

PROFESSOR BLAKEY: Was this the wife of the Mayor?

MR. ERTEL: This was the Mayor, himself.

PROFESSOR BLAKEY: No, whose wife?

MR. ERTEL: The wife of the Director of Public Services, who was responsible to the Mayor. We had three department heads responsible to the Mayor and she disclosed the entire conversation. So you see we had both the co-conspirator talking and also a stupid move, which gave us enough evidence without any other things to go forward in our prosecution.

I think I have covered generally what happened.

I might point out one other thing. I said there was difficulty in getting a conviction. The defense in the case was these people were trying to do their function, get corruption in the city government. The only trouble was that in the trial the people the Mayor said were corrupt were the people he just appointed. So it doesn't follow he would appoint corrupt people and listen in on their phone calls.

The defense was attempted to be inserted but never got off the ground because the Mayor never took the stand himself. So trying to insert a defense without your principal getting on the stand certainly was difficult.

The third thing is if, in fact, that trial had been held in his own jurisdiction—they moved for a change of venue which we did not forcibly attempt to prevent. In other words, we did not put up a strong defense to a change of venue. By moving himself to another area he certainly did not have the sympathy of his particular group on the jury. So we got an impartial jury. I think the Commonwealth came out better as a result of the change of jurisdiction. If we had tried it in his jurisdiction we probably would have had a hung jury.

So I think it's very difficult to get a conviction in a wiretap situation where there are public officials involved. I think it would have been better for the United States Government to have done the prosecution because then it becomes more removed from the public arena.

I am an elected public official and immediately they can make the accusation that this is a political hassle rather than a legitimate criminal prosecution. I don't believe that but they can certainly make that allegation and try to present it to a jury.

And it would have been better had the FBI, through the United States Attorney's Office, prosecuted this case.

I think I have given you pretty much the background of the cases.

I might point out a couple of things I considered about the federal law which I thought were unusual.

One thing I dispute in the federal law is you have an emergency provision which allows wiretapping in what is called, quote, emergency situations, and you can later go to the courts within 48 hours and get retroactive application or permission to do it.

I think the case in Williamsport shows that once you have obtained some sort of information of a wiretap, it is a temptation to use what you have already obtained and revert it back to your probable cause and attempt to justify your emergency situation by what you have obtained. I don't think there is any need for that. I think it leads to the possibility of abuse.

I do not see why you could not get a judicial warrant in any situation where you need wiretapping, why there is ever an emergency situation. Certainly you have some information prior to that which will allow you to get a warrant and you do not need to justify it after the fact.

CHAIRMAN ERICKSON: You feel that the emergency provision as it is presently constituted, which we must tell you we are advised has not been individually used, is constitutional?

MR. ERTEL: I would think it would not be. I would certainly attack it on that ground.

CHAIRMAN ERICKSON: On what ground would you attack it?

MR. ERTEL: On the grounds that really it is an invasion of privacy under the rubric of search and seizure, even though it is outside your home. That rubric has gone much further to protect your right of privacy and therefore you are doing it without judicial permission, without a warrant.

I think the *Katz* case might be a case which might have some implications.

CHAIRMAN ERICKSON: A touchstone.

MR. ERTEL: I would start with that as my original premise and argue from that.

It may not be widely used, but I think the temptation is there and I think it can be abused.

But I do believe you need the one-party consent to the interception of telephone calls. I think that is necessary. I think it is proper. Because no one has the right to expect privacy. If I speak to you I have to recognize that you may go and broadcast that conversation, whether you do it with a recording or just through your word of mouth.

Secondly, I think the same thing happens on the telephone. Whether it is a wire communication or oral communication, I think it is necessary and the federal law is correct. The Pennsylvania law is not. And the judicial warrant should be from a court of record for any sort of wiretapping, I think.

I really have concluded most of the things I have to discuss. I would really like to answer any questions I can for you.

CHAIRMAN ERICKSON: Mr. Hershman of the staff will conduct the interrogation.

MR. HERSHMAN: Thank you, Mr. Ertel. You have covered the Williamsport situation so thoroughly I have but a few questions.

You mentioned you had found some equipment in City Hall. Were you ever able to determine where the equipment was obtained?

MR. ERTEL: Well, there are two sets of equipment that we were referring to. Number one was the equipment which had previously been in the city police department. That equipment was obtained probably in 1967 through an organization in the state of New Jersey. The name I do not have with me but I could supply it. We were able to trace that.

As far as the equipment we could conclusively prove was used in the wiretapping in the City of

Williamsport—at least in my judgment conclusively prove—was equipment obtained from the Bell Telephone Company itself.

Bell Telephone has—and I have some pictures I would be glad to let the Commission see which were left over from the trial. Bell Telephone has certain rooms in buildings such as this building, any government building, any major office building, any complex. It is their telephone room. In that room they have what is called a butt-in device. That is a shorthand term for a telephone repairman's instrument. It looks like a telephone. You have probably seen them on any telephone repairman who comes into your home. He plugs into a circuit and uses it to see if the circuit is working.

This is a perfect wiretapping device because, properly inserted and hooked up, there is no diminishment of sound on the line whatever, and you have perfect, crystal-clear communication between the two parties to the communication. This device does not give any echo or sound over the system and you can sit there and listen in if you can get to a terminal box or any exposure to the wires. You can also put an amplifier on that and do it at a distance.

The device costs about \$13 to \$15, I am informed.

They are sold on the market but also Bell Telephone installs one of these portable pieces of equipment—doesn't install it, has it there—in all these telephone rooms in public buildings. So all you have to do is get in and listen in on any conversation you want once you have access to the wires.

In that particular building, since these offices are very secluded and very seldom entered, you can sit right there and monitor any phone call you want. And usually they have a book right in the room itself which lists various numbers—for instance, "Circuit XY"—and I am not certain they are letters—"goes to Jim Doak's office or Jim Doak's home."

You just go to XY and plug in and you have a perfect intercept. They even have a nice little chair and desk so you can sit there and make a log as you go.

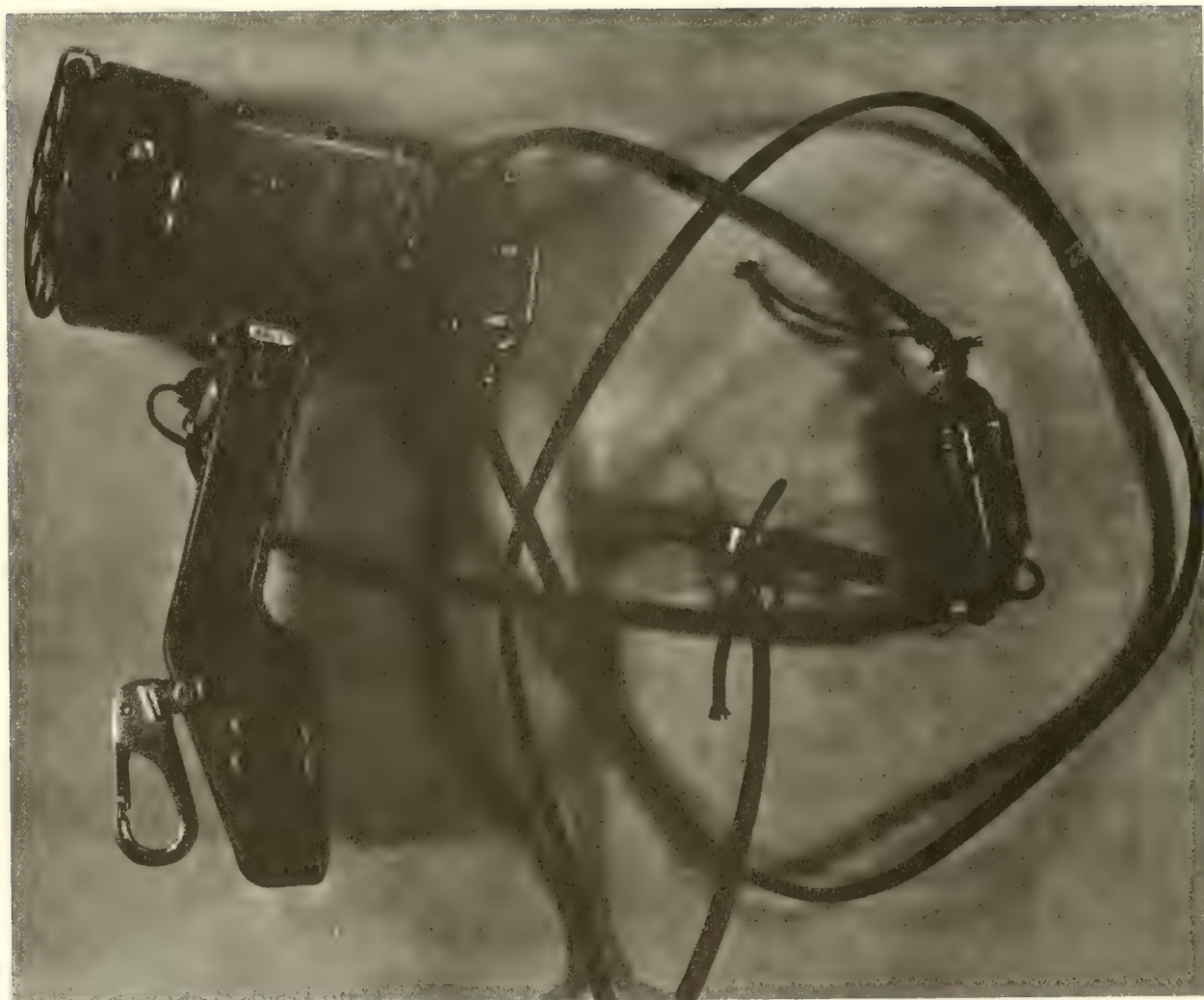
MR. HERSHMAN: I wonder, Mr. Ertel, if we could enter those pictures into the record at this time.

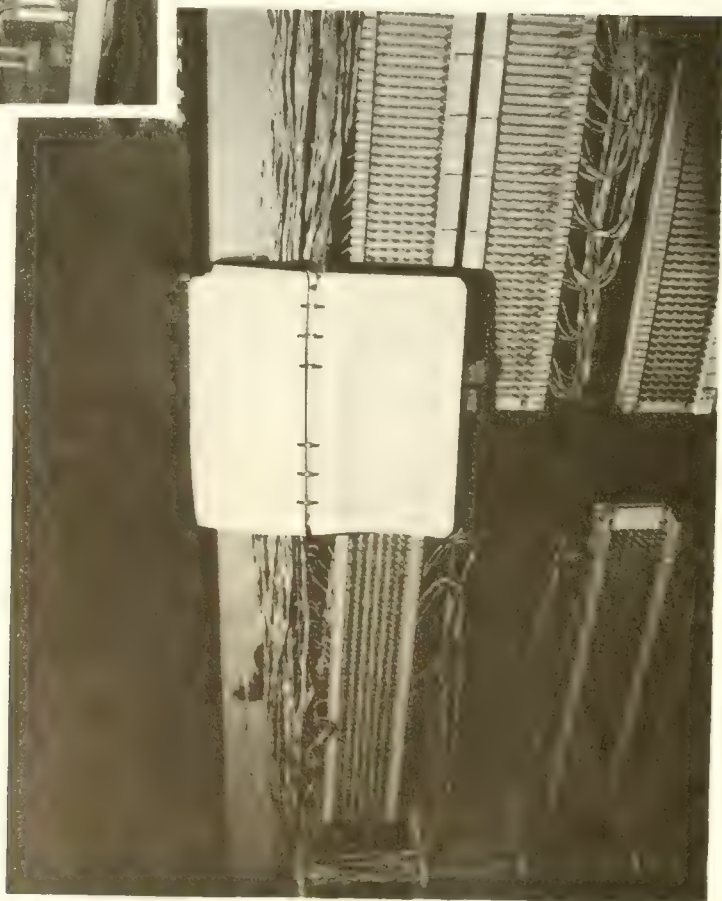
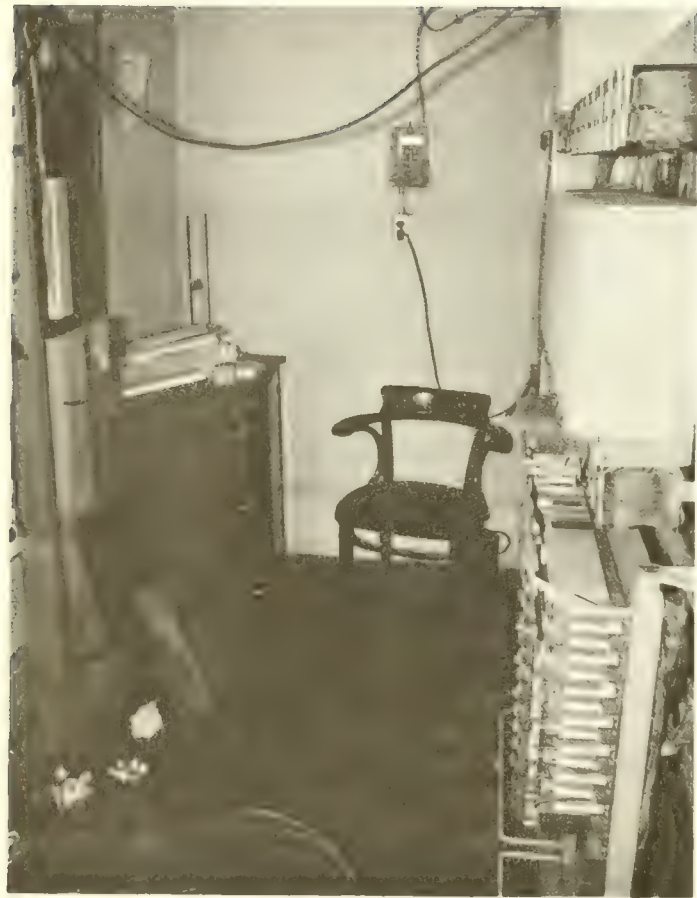
MR. ERTEL: Surely, You have to forgive them. They have Commonwealth numbers on them.

[The material referred to follows.]











MR. HERSHMAN: And you say, Mr. Ertel, that these devices, some of them, were obtained from the Bell Telephone Company?

MR. ERTEL: Yes.

Number one, I have four color photographs which show the room and the chair itself, with the panel for the entire transmission in the City Hall.

They even carry the book and I have a picture of the book open to a page which you cannot read, which gives you the nomenclature.

What has been marked as Commonwealth's Exhibit 5 in the previous trial shows the device itself and how it can be used. This was taken directly from the Bell Telephone room. And the evidence in our case showed that at least this type of device was used.

There are a couple of those photographs here.

CHAIRMAN ERICKSON: Mr. Ertel, was most of the monitoring done from this particular room in City Hall?

MR. ERTEL: I can't answer that question. One could suspect that some was done there. We had no conclusive evidence of it.

The room was available. It was allegedly locked but according to the testimony it was not.

In our particular case there was a special extension put on a phone from the one person whose phone was to be tapped, the Captain of the Police, and run up to the Public Safety Office.

That was put in by the Bell Telephone Company, itself, under conditions of secrecy. They agreed to do it secretly. And they did it secretly and put that extension in without notifying anybody else. And then they used the butt-in device off that circuit coming up with a tape recorder.

In the other instances it was hooked directly into the lines right in the Mayor's office. He would hook into the line because it came into his office.

MR. HERSHMAN: Was there any complicity found on the part of any Bell Telephone Company employees?

MR. ERTEL: We charged a Bell Telephone Company employee who had allegedly delivered a butt-in device to the Mayor of the City of Williamsport who was a friend of his who was nominated to a public post. He was put on a special probation program in the State of Pennsylvania and has now been discharged. His only role, as we could determine it, was delivery of one of these butt-in devices to the Mayor himself.

MR. HERSHMAN: Did you find that the individuals implementing the wiretaps had any special training in that area?

MR. ERTEL: The Director of Public Safety of the City of Williamsport had previously been a Bell Telephone employee. He had approximately five

years of service with Bell Telephone in California. So that he did have, I would say, extensive experience in the use of telephone and telephone equipment.

One of the officers who had testified at the trial, who did not directly do any wiretapping, had been trained to wiretapping by the FBI, and went to the FBI school.

MR. HERSHMAN: Mr. Ertel, you testified that the State Police were originally reluctant to become involved. Why was that?

MR. ERTEL: Well, I didn't say initially. I would say at the operational level they were not—and up through the Regional Commander.

When we reached the Commissioner of the Pennsylvania State Police, who is the statewide head of the State Police, that is where the difficulty arose.

I have never had a satisfactory explanation of that decision, and I have talked to both the Deputy Commissioner and the Commissioner concerning it. I cannot give you their reasons.

One can surmise, but I cannot give you their direct reasoning.

MR. HERSHMAN: And you also stated that there came a time when the Mayor and the Director of Public Safety took an illegal wiretap tape to the offices of the FBI in Williamsport; is that correct, sir?

MR. ERTEL: That is correct.

MR. HERSHMAN: Did you have discussions with FBI agents about the conversation that took place at that time?

MR. ERTEL: I did. And they also testified at the trial of Mayor Coder and also testified at the trial of the Director of Public Safety.

Quite frankly, their reasoning was that they accepted at face value the Mayor's statement that this was an inadvertent thing, and I suppose they considered it de minimus.

I understand your problem—

MR. HERSHMAN: It was on tape and it was the beginning of the conversation to the very end; is that correct?

MR. ERTEL: That was my impression, yes.

MR. HERSHMAN: And they accepted at face value the statement that it was made inadvertently?

MR. ERTEL: I think they considered it de minimus, that is, of not sufficient importance. They did advise him to stop it. I would question the judgment, but I think they did it in good faith.

But there was no follow-up.

Incidentally, I did request through one agent whether or not the United States Government was going to prosecute this particular case, because obviously I had been disclosing along the line most of

what I had been learning to the FBI. And I was advised that they did not intend to take any action.

MR. HERSHMAN: Did they in fact—

MR. ERTEL: That came from the United States Attorney's Office allegedly.

MR. HERSHMAN: So they did, in fact, go to the United States Attorney's Office? Is that correct?

MR. ERTEL: That is the information that was given to me.

MR. HERSHMAN: By whom?

MR. ERTEL: By the agent. I have never discussed it directly with the United States Attorney. We intended to go forward at that point, because we were so far down the line. It may have been a judgment based on the fact that two jurisdictions cannot prosecute for the same crime under Supreme Court decisions.

MR. HERSHMAN: Mr. Ertel, did it appear to you that the FBI agents were familiar with the provisions of the Federal Wiretap Act?

MR. ERTEL: Yes, I think they were. I don't see any reason they would not be. One was the man in charge of the Organized Crime Division; and, secondly, I had sworn out an affidavit for this particular FBI office to obtain a legal wiretap, a judicial wiretap under the Omnibus Crime Act, so I am certain the FBI was quite familiar with the Act itself.

And that was prior to this.

MR. HERSHMAN: In the letter you have addressed to the Commission you state as follows:

"As is readily apparent, when a police agency under the authority of its top officer embarks on a course of illegal conduct, other police agencies are reluctant to become involved."

I wonder if you would comment on that.

MR. ERTEL: Well, quite frankly, I think my experience with the Pennsylvania State Police at the Commissioner's level indicated they were reluctant to become involved because they knew another police agency was involved. They knew a police captain was involved, who was one of the conspirators. They knew the Director of Public Safety was involved, who was in charge of the police department. And I think they became reluctant to become involved in a particular prosecution.

I think this is common among any police agencies, that they tend to protect themselves in a way. I think they are reluctant to get into an inter-police squabble, if you want to call it that.

MR. HERSHMAN: Mr. Ertel, the Mayor of Williamsport has been quoted as saying:

"Every phone in every public building should be tapped in the interest of bringing an end to a lot of corruption."

Does that accurately reflect his attitude?

MR. ERTEL: I don't know if he made that direct quote. I was not present so I would not want to say that. I think, as you indicated, that is his attitude; I think that is correct.

I think he feels, unjustifiably so, that he is powerful enough as a city official that he is entitled to listen in to anybody's conversations at any time, and that he has that right and authority to do so, regardless of who it is or what it is.

And he had made that quite clear.

I did take the statement of the Mayor of the City of Williamsport under oath, at his request, and I might point out at that time his attorney, a very honorable gentleman, asked me to do that, thinking this was only a de minimus situation, and I would say "Don't do it any more," and forget it.

At the end of the deposition, the attorney turned to me—and it is in the transcript—"Well, Al, I hope you've got it all now. He certainly told you more than he told me," which would indicate to me the attorney had not been fully aware of the implications, because I had the conversations and the tapping other than just the one isolated incident they had been talking to me about. So I think that is the view of that particular individual.

MR. HERSHMAN: Just one further question, sir. In your conversations with the Federal Bureau of Investigation or the United States Attorney's office, did you ever make it clear that this case would have been best prosecuted under the federal statute?

MR. ERTEL: No, I did not. That would be an unfair statement to anyone involved.

I had conversations only with the FBI and did not converse directly with the United States Attorney—I'm sorry; on one occasion I did talk directly to the United States Attorney's office.

But I made it clear that we would go forward and that we were not going to allow it to happen in the City of Williamsport or Lycoming County.

I asked them if they were going to prosecute and what their position was, but I did not say to them directly, "I feel it is better that you do it." Because we had the information at that point, and I never said to them "You prosecute." No, I did not say that.

MR. HERSHMAN: So they were aware that justice would be done?

MR. ERTEL: Assuming that justice was done, and I think it was, yes, I think they were aware we were going to go forward. Although there are certain criminal acts which are criminal under the federal statute which were done during this period of time which were not criminal under state laws which have not been prosecuted.

MR. HERSHMAN: Thank you.

CHAIRMAN ERICKSON: Thank you, Mr. Hershman.

Judge Pierce?

MR. PIERCE: I have no questions.

CHAIRMAN ERICKSON: Judge Shientag.

MS. SHIENTAG: Thank you, Mr. Chairman.

I note that you are a district attorney at the same time that you practice law.

MR. ERTEL: Right.

MS. SHIENTAG: That is permissible in your community?

MR. ERTEL: That is permissible in the State of Pennsylvania outside of the major metropolitan areas. The only one I know that is full time is the Philadelphia District Attorney's office. All the rest of us are part-time prosecutors.

MS. SHIENTAG: And it is an elective office?

MR. ERTEL: We are.

MS. SHIENTAG: Was there ever any interference with your duty as prosecutor?

MR. ERTEL: You mean through my private practice?

MS. SHIENTAG: Let me rephrase that.

By virtue of the wiretaps while you were prosecutor, was there ever any interference with the discharge of your duties as prosecutor?

MR. ERTEL: That is difficult to say. I think that we may have had some. Evidently the suspicion of wiretapping and overhearing, in other words, bugging devices within the City Hall and police department, was widespread before I became aware of it.

And these officers refused to talk on the telephone. When I would talk to them they would come to my office.

There were confidential narcotics investigations going on, which one investigator felt had been leaked because he had good information as to the narcotics movement and all of a sudden things changed.

Incidentally, that police officer has left the city police department and has now gone to the State Department of Narcotics Control.

MS. SHIENTAG: I see. Was the wiretapping conducted only in your official District Attorney's Office or did it transpire in your private law office?

MR. ERTEL: No, no. I might have misinformed you. But the wiretapping physically took place in the City Hall, not in my offices.

MS. SHIENTAG: You never had that in your office?

MR. ERTEL: Not that I am aware of. I have no evidence that there was any wiretap.

MS. SHIENTAG: So there was never any attempt to infringe on the rights of your clients, vis-a-vis you as their attorney?

MR. ERTEL: No, I doubt that very much.

MS. SHIENTAG: Now, you testified that you confronted the Mayor's attorney at a meeting with certain tapes and he said "You know more than I do."

MR. ERTEL: If I inferred I had tapes—information, not tapes. I never had any tapes. I had more information, because I had derived the information from my investigation and had all of this knowledge at my disposal. When I interrogated the Mayor with his attorney present, at his request, I would ask him "Is there anything further that you know about wiretapping?" and I would get a sort of numb response of "No."

And I would suggest another area where the wiretapping may have taken place, and then I would get the information.

It was sort of like a cat and mouse game, if you will.

MS. SHIENTAG: In the State of Pennsylvania there may not be any wiretapping for prosecutive purposes; is that correct?

MR. ERTEL: That is correct.

MS. SHIENTAG: Except for the protection of the officer?

MR. ERTEL: That particular provision, as I understand it—as I read the Code, there are two different sections of the Code. One section of the Code says "No wiretapping at all."

Under the eavesdropping section, which is the amendment passed in December, effective in February of this year, you may bug a police officer for his personal safety, and that's all. And you can do that if you have reason to believe that his life is in jeopardy—in other words, to bring assistance to him.

MS. SHIENTAG: Isn't that consensual wiretapping?

MR. ERTEL: I distinguish between that and wiretapping. Wiretapping is the interference between wire communication—

MS. SHIENTAG: You are referring to a body recorder?

MR. ERTEL: Body mike or body recorder.

MS. SHIENTAG: That is not prohibited?

MR. ERTEL: It is prohibited. It is prohibited to do it unless the personal safety of the officer is involved. And you tell me when the personal safety of an officer is involved. Is it involved all the time in his investigation, or is it when he is going into a very specific situation where he knows he can be hurt?

I think it is a very ambiguous section.

MS. SHIENTAG: And therefore subject to the misdemeanor prohibitions at the peril of the officer carrying the recorder.

MR. ERTEL: That is very much so. In fact, we just completed an extensive narcotics investigation with 40-some arrests. At no time did we use anybody mikes even though the man was probably in jeopardy at times, because the officer would not take the chance.

MS. SHIENTAG: Thank you very much.

CHAIRMAN ERICKSON: Chief Andersen.

CHIEF ANDERSEN: Mr. Ertel, you said in your testimony the Mayor put an extension up to somebody's office, which is illegal in Pennsylvania.

MR. ERTEL: Right.

CHIEF ANDERSEN: My question is: How did you handle extension phones in public buildings in Pennsylvania? Do you have extension phones?

MR. ERTEL: Sure.

CHIEF ANDERSEN: How do you do it?

MR. ERTEL: You don't put them in secretly. People know they are in existence, that they are an extension over your phone.

For instance, we publish a directory. The directory says Extension 353, for instance, goes into XY's office. If somebody picks up the phone inadvertently and puts it back down, I do not consider that a wiretap. But what he did is he had the extension run up. Then he attached one of these butt-in devices to the wall outlets.

I am not a wiretapper so I have to rely on what somebody else tells me.

CHIEF ANDERSEN: Yes.

MR. ERTEL: There are two lead-ins or terminals. From those you might hook on this extension.

If you pick up an extension telephone, the other person knows that you have done it. They hear the click. It is an audible sound.

Or if you have the button-type arrangement on your phones, the light may come on if he picks up before you do, or hangs up after you. You can see the light on the phone. So the person is aware that there is somebody on the other phone.

And also, one knows in an extension telephone one can expect somebody can pick up the extension and listen in. Your expectation of privacy is more limited.

The phone that was tapped in this particular instance was a one-instrument telephone. In other words, there was one instrument in the City Hall. There was a confidential line put in for the investigation of drugs and gambling, which was used generally for informers calling in, or for a very confidential source. This was not the ordinary telephone like you might have in your office and your secretary might have in her foyer and she dials you up and says "Take Line 3," or whatever it might be.

This was a one-instrument phone in the one instance.

In the other instance, it was the multiple-extension phone.

CHIEF ANDERSEN: What you are saying is that in public buildings every phone that has an extension must be listed in the directory basically?

MR. ERTEL: I am not saying that. I think it would be a practical solution. It doesn't have to be by law, but certainly if you want to dial somebody up you have a directory to dial them. But the point is that you do not sit there and monitor somebody else's phone calls which are coming in through his extension phone.

Would you like it if your secretary, who was working for somebody else in the administration, sat there and recorded every one of your phone calls and gave it to the person in the administration? And that is what was happening.

CHIEF ANDERSEN: I have no more questions.

MR. ERTEL: I hope I have been clear.

CHIEF ANDERSEN: I still don't understand it. It bothers me.

MR. ERTEL: Okay. If I can answer any further questions, I would be happy to try.

CHIEF ANDERSEN: No, I don't think you can. I think it is the statute.

CHAIRMAN ERICKSON: Mr. Blakey.

PROFESSOR BLAKEY: Mr. Ertel, let's see if I can figure it out. He had an extension run from upstairs down to the basement room?

MR. ERTEL: Right.

PROFESSOR BLAKEY: And the phone company came and gave you this extra wire?

MR. ERTEL: They put it in.

PROFESSOR BLAKEY: It wasn't like an extension. It was a leased line.

MR. ERTEL: Right.

PROFESSOR BLAKEY: Instead of having to go downstairs to that little room and listen on a head set he could hook it up and sit and listen in the comfort of his room. It really wasn't an extension.

MR. ERTEL: No, it wasn't serving that function. It was ordered as an extension telephone under the guise of being that. The wires were run by the Bell Telephone secretly. They were run from the basement which was the City Police Department, off this private line to the second floor. There they used the butt-in device.

In other words, it is just an extension of the butt-in device, if you want to call it that. The physical fact is there were lines that were installed.

PROFESSOR BLAKEY: Mr. Ertel, I only have one or two questions but I would like to say that I found your testimony very helpful for figuring out some of the practical problems with wiretapping.

Let me question you a little bit about just one issue.

How long have you been a District Attorney?

MR. ERTEL: I am in my 8th year.

PROFESSOR BLAKEY: Your 8th year?

MR. ERTEL: Yes.

PROFESSOR BLAKEY: And you are part time?

MR. ERTEL: Yes, supposedly.

PROFESSOR BLAKEY: About how much of your time is spent in the office?

MR. ERTEL: Well, percentagewise, a great deal. I have never clocked it. I spend at least 40 hours a week. I usually put in a 60- to 70-hour week. So it is very difficult to measure.

For instance, last week I tried a murder case and I started at nine in the morning and our judge ran till nine o'clock at night.

PROFESSOR BLAKEY: And you did it in a day?

MR. ERTEL: No, we did it all week, for five days. So we put in a pretty good working day.

PROFESSOR BLAKEY: How large is the county you serve?

MR. ERTEL: It is 120,000 or 130,000 people.

PROFESSOR BLAKEY: Do you have any investigators assigned to your office?

MR. ERTEL: I have one who is called a County Detective. Basically he winds up serving subpoenas—just filling in loose ends—and getting cases ready for trial. He is basically the man we rely on. He does no investigating as such. He is strictly a process server, administrative yeoman, everything you can think of.

PROFESSOR BLAKEY: Is your role essentially that of a courtroom advocate?

MR. ERTEL: Yes. I would say we advise police departments on investigations. We consult with police departments in almost every investigation. Every narcotics investigation is reviewed by us, and murder cases, also. But in the general run of things, we are not an investigating agency; we are reviewing.

PROFESSOR BLAKEY: Do you have an investigative grand jury available to you?

MR. ERTEL: In Pennsylvania there are very strict ways of procedures for getting an investigative grand jury. We had one in this particular case. We must allege and be able to establish, number one, criminal activity.

PROFESSOR BLAKEY: To begin with?

MR. ERTEL: To begin with. It is very difficult to get a special investigating grand jury. There are many cases I am sure your counsel is aware of that came out of Philadelphia. But you must have widespread criminal activity and have special process of law. And in this case, because of the extent of the wiretapping that we knew of and the fact

the government, itself, was involved, we were able to get a special grand jury impaneled.

PROFESSOR BLAKEY: You don't have any extensive experience in organized crime investigation, do you?

MR. ERTEL: No.

PROFESSOR BLAKEY: So I take it that your judgment that you don't need emergency surveillance is that you really haven't seen any need for it in your experience.

MR. ERTEL: Well, I have sworn out some affidavits allegedly about organized crime. I have reviewed some organized crime activities for some other agencies. I have discussed it with others.

That is why my view is what I have.

PROFESSOR BLAKEY: What I am raising with you is that we have had testimony from the Drug Administration, the Federal Bureau of Investigation, even examples from the New Jersey State Police, of dynamic investigation or situations where they thought the emergency power—I am not speaking now about constitutionality—they felt the emergency power was necessary; there was no time to get to a magistrate.

And I am just trying to see what the relationship between your experience and theirs is.

What I am saying is: You seem to be very capable and very knowledgeable about what you are doing. But I am just wondering whether you had the same kind of experiences that they have had, and consequently would be in a position to make the sort of judgment that they did.

MR. ERTEL: Well, quite frankly, we have not investigated organized crime except what might purport to be one case, where I executed affidavits for the Organized Crime Division of the FBI. We have cooperated in those investigations, also with the State of New Jersey. In fact, one of the individuals they consider to be one of their organized crime figures we convicted in our county on another charge.

PROFESSOR BLAKEY: Your judgment that it might be unconstitutional—

MR. ERTEL: That is a question for the Supreme Court.

PROFESSOR BLAKEY: That is for somebody else to decide. Your judgment, however, is that it might be abused. That, I think, is one that certainly could be held without much quarrel. But your statement is that it isn't needed. That is a factual matter, isn't it?

MR. ERTEL: That is a factual matter which I am sure there is quite a bit of dispute on.

And the same factual dispute is we need to search in certain instances without a warrant. Certainly we have had a lot of experience with that.

And generally in most cases you can get a warrant. There are extenuating circumstances.

PROFESSOR BLAKEY: Thank you very much, Mr. Ertel. I appreciate that.

CHAIRMAN ERICKSON: Professor Blakey has stolen about ten of the questions I intended to ask, so I am in a position where I am just going to let you fill in a few of the things that he didn't quite go into as far as I would like to get the information.

When it comes to the investigation of this wiretap, you didn't use the investigator in your office. You said you have one investigator.

MR. ERTEL: Yes.

CHAIRMAN ERICKSON: The investigation was made by the Pennsylvania State Police after you contacted the Governor?

MR. ERTEL: Correct.

CHAIRMAN ERICKSON: In Pennsylvania, by reason of your law, and particularly prior to your new eavesdropping law, you could not even use a consensual or body mike when it came to law enforcement personnel under any circumstances?

MR. ERTEL: I think you have turned that around.

CHAIRMAN ERICKSON: Well, perhaps I can rephrase it. Let me put it this way—

MR. ERTEL: The body mike cannot be used today. Prior to February, the body mike could be used.

CHAIRMAN ERICKSON: It can't be used at all today?

MR. ERTEL: Not at all. It is absolutely prohibited except for personal safety. But prior to February of 1975, the body mike was able to be used and was used extensively.

CHAIRMAN ERICKSON: All right. I did have that turned around and I am glad you straightened me out on it.

Now, this law that you have in Pennsylvania that does put the prohibition on body mikes—

MR. ERTEL: Right.

CHAIRMAN ERICKSON: —has that had any effect on the use of them in the federal courts, so far as you know? Are they still using them in federal courts?

MR. ERTEL: That is a legal issue. The Pennsylvania statute says it is not admissible in any legal proceeding. I suppose that is procedural, since evidence is generally considered procedural under the federal rule. And I would think that you can still probably use those in a federal court even though the Pennsylvania courts would not use it.

But that is a legal judgment which could be tested in the courtroom and I do not know if it has been tested.

We, incidentally, are on appeal in that particular situation to the Pennsylvania Supreme Court with the use of a body mike.

CHAIRMAN ERICKSON: I think it would be a fair statement, from some information that we have, to say that wiretapping is as hot an issue in Pennsylvania as it is in most places; isn't that true?

MR. ERTEL: At least from our press I could consider it to be a hot issue, and we certainly looked into a lot of other cases before we brought ours.

CHAIRMAN ERICKSON: As a matter of fact, you have had a Commission at work for some period of time. One of our former staff members, Downey Rice, has been working with the State of Pennsylvania. What has that Commission been doing?

MR. ERTEL: They have held hearings in Harrisburg. The House of Representatives has a committee. Allegedly they were extensively involved in the King of Prussia wiretapping where it was alleged state police were tapping other state police. And that was for an extended period of time.

I don't know that they have come up with any legislation. And if the legislation they did come up with was this eavesdropping act, I would suggest it was improper legislation.

CHAIRMAN ERICKSON: Well, I thank you very much for your testimony. You have been quite helpful. The problem that we have is to review not only federal but state laws on wiretapping. Of course, the purpose this Commission has is to view and determine what has occurred since the Omnibus Crime Control and Safe Streets Act came into existence, to determine whether this has been the tool that affected good law enforcement and made it possible to carry that out, and whether that was done at the expense of the right of privacy or whether privacy was protected in the same act. And you have been very helpful.

MR. ERTEL: Thank you very much.

[Material relevant to Mr. Ertel's testimony follows.]

District Attorney's Office

COURT HOUSE

WILLIAMSPORT, PENNSYLVANIA

May 15, 1975

Kenneth J. Hodson, Executive Director
National Commission for the Review of Federal & State Laws
Relating to Wiretapping and Electronic Surveillance
1875 Connecticut Avenue N.W.
Washington, D. C. 20009

Dear Mr. Hodson:

In regard to your invitation to appear before the Commission on Wiretapping and Electronic Surveillance, I would be happy to appear. My biographical background is attached hereto.

Turning to the questions framed in your letter, it would be impossible to recite all the background of the cases involved in the Williamsport Wiretapping situation. In these cases, it was the District Attorney's Office's position that Mayor Coder was tapping these phones for his political purposes, especially in view of the fact that he played the tapes at his home to a person who had been discussed in the telephone conversation. The conversations were between individuals who did not realize their conversations were being intercepted. In the Coder case, we suspected, but were not able to prove, that many more telephones were tapped than actually were proven in the prosecution. The reasons for this belief are too numerous to relate at the present time. Actually interceptions proven or admitted to amounted to approximately 50 to 60 different calls. In all instances of wiretapping, the person who was in overall command of them was the Mayor of the City of Williamsport. This, in and of itself, made it difficult to prove our case since the persons doing the actual operation were under the thumb of the Mayor for their livelihood. In addition to that, they were police officers and the Director of Public Safety of the City of Williamsport, which made it difficult to investigate the situation. No cooperation could be expected from the City Police Department since its Director and some officers were involved, including a Captain in the Department. Fortunately, most officers did cooperate with the investigation once they knew of the investigation, even though they knew their jobs were in jeopardy. I found it necessary to enlist the support of the Pennsylvania State Police to investigate the matter and even this was difficult because of the involvement of the Mayor and Director of Public Safety. Initially, at the level up to Regional Commander, the cooperation was excellent; however, the Pennsylvania State Police Commissioner's Office withdrew the offer of assistance by the Regional Commander allegedly because of the implications of the case. This decision was reversed the same day after I personally called the Governor's Office to insist that the investigation should be handled as any other criminal investigation.

Upon initial contact with the F.B.I., specifically, Charles K. Fahien, I had excellent cooperation. At that time Mr. Fahien advised me that Mayor Coder and Director of Public Safety Samony had been to the F.B.I. with a tape recording an alleged phone conversation between Ernest DePasqua, a Police Captain, and another person. Mr. Fahien advised me and subsequently testified that the Mayor and Samony implied that this was an inadvertent overhearing on an extension phone and a recording when the content of the conversation was known. Although this was a violation of the Federal Law in my opinion, as the matter was explained to the two F.B.I. Agents, they considered it de minimis. At least six months' later, an unsubstantiated complaint was made to the F.B.I. concerning the Mayor's overhearing telephone conversations; however, this alleged incident was not considered to be related to the first.

Subsequently, I informed the F.B.I. of my information concerning wiretapping at City Hall for their consideration and some time later I was informed that the U.S. Attorney's Office was not going to prosecute. I cannot tell, nor do I know, the reason for this decision, although it may have been that they knew at this time that my office, along with the Pennsylvania State Police was investigating the allegations. I might also add that the Mayor told the F.B.I. that he thought his life was being threatened in the recorded phone call he took to the F.B.I. The F.B.I., as well as myself, considered this allegation to be meritless and really considered the phone call to be a political move by the parties involved. The trip to the F.B.I. by the Mayor, in my judgment, was also politically motivated. Incidentally, the recitation by Mayor Coder of the means of the interception resulted in a criminal charge because he later stated that this was a deliberate tap and not inadvertent.

I hope this limited background can be of assistance to you. As is readily apparent, when a police agency under the authority of

its top officer embarks on a course of illegal conduct, other police agencies are reluctant to become involved. This becomes a very real danger unless independent agencies intervene. The danger is not only of the immediate invasion of privacy, but the long term effects. When these top officials once become compromised, they are subject to further compromise by implied threats and can become wholly lawless. Also once one embarks on the road of being lawless while in office, it is contagious to others, especially those in government.

Turning briefly to the difficulties of prosecuting these cases, it is obvious from the above recitation that it is difficult to obtain proof of the crimes themselves. As in any crime of stealth, the discovery of the incident itself is difficult. Unless a participant talks, or a stupid move is made by the wiretappers, the crime itself will go undetected. Even if one of the participants does confess and testify, it then normally becomes an issue of credibility as to that witness whose motivation in testifying can be attacked. To buttress a testifying participant, it is usually helpful to have physical evidence like tapes, transcripts, or the equipment. Generally by the time you obtain a party to testify, the criminal defendants know of the investigation and this material is destroyed. Consequently, the factual proof of illegal wiretapping is difficult to obtain.

The statutes themselves are not difficult of interpretation, however, the Pennsylvania State Statute may be too broad in scope and the Federal Statute, as a result of judicial interpretation, too narrow, to effectuate a policy of protecting against the invasion of privacy of an individual while also preventing the Statute from becoming an effective assistance in law enforcement. The Pennsylvania Anti Wiretap Law, prior to the recent newly enacted electronic surveillance Statute which will be discussed subsequently, prevented any listening in on conversations by telephone if both parties did not agree. In effect, no interception for law enforcement under any circumstances. Law enforcement authorities could not even get a warrant to intercept upon probable cause nor with the permission of one party to the conversation. Thus, if a police informer is on one end of a conversation he cannot allow another to listen in on it or record it even if a crime is being planned. No one could reasonably expect privacy in such a conversation since one party could disclose it. Also, if the police can search a home or other dwelling with a search warrant upon probable cause, should not a policeman be entitled upon probable cause with a warrant issued by an independent judicial authority to listen to telephone conversations. Both situations are invasions of some privacy based upon probable cause determined by a judicial authority; however, Pennsylvania Law prohibits such actions. The newly enacted Pennsylvania Statute on electronic eavesdropping is so restrictive that one could call it not a "right to privacy" statute, but a "right to corrupt" statute. The reasons for such an opinion are extensive and I will not recite them here.

As to the Federal Statute, it allows interceptions with one party's consent and also by judicial warrant. However, by judicial interpretation, prior to the Omnibus Crime Act, it allowed a "superior right interception" by a subscriber. I consider such a position to be generally meritless, and also repealed by the Omnibus Crime Act; nevertheless, this should be statutorily put to rest.

In my opinion the Williamsport activities were in violation of both the Federal and State Laws even though no Federal actions were brought. This also may be the result of recent case law which precludes two jurisdiction from convicting for the same acts.

To discuss these statutes in more detail would require an extensive dissertation. I hope this suffices to acquaint you with my positions on these matters.

Very truly yours,

[Signed]
ALLEN E. ERTLE

CHAIRMAN ERICKSON: We now call Mr. Jerry Schneider.

[Whereupon, Mr. Jerry Schneider was duly sworn by the Chairman.]

CHAIRMAN ERICKSON: Mr. Schneider, we are very pleased to have you with us today. Mr. Schneider is the president of Jerry Schneider & Company, an organization formed in 1972 which specializes in providing security systems for compu-

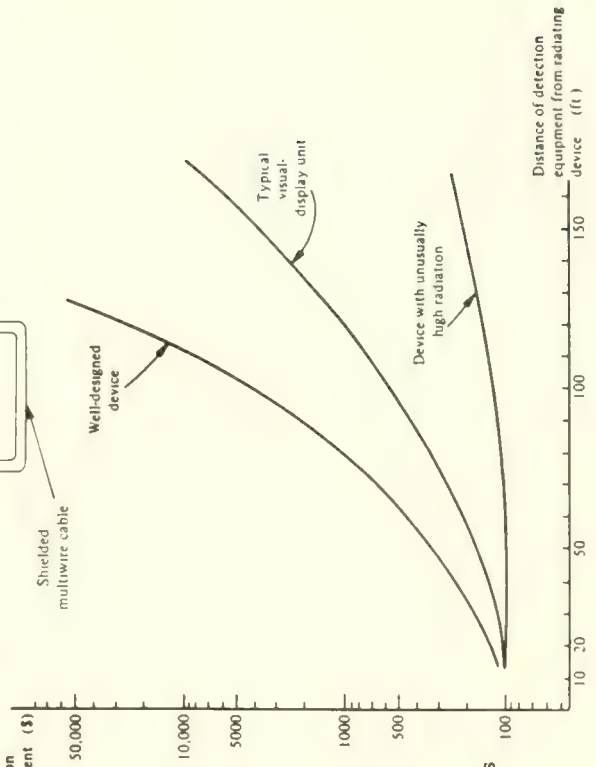
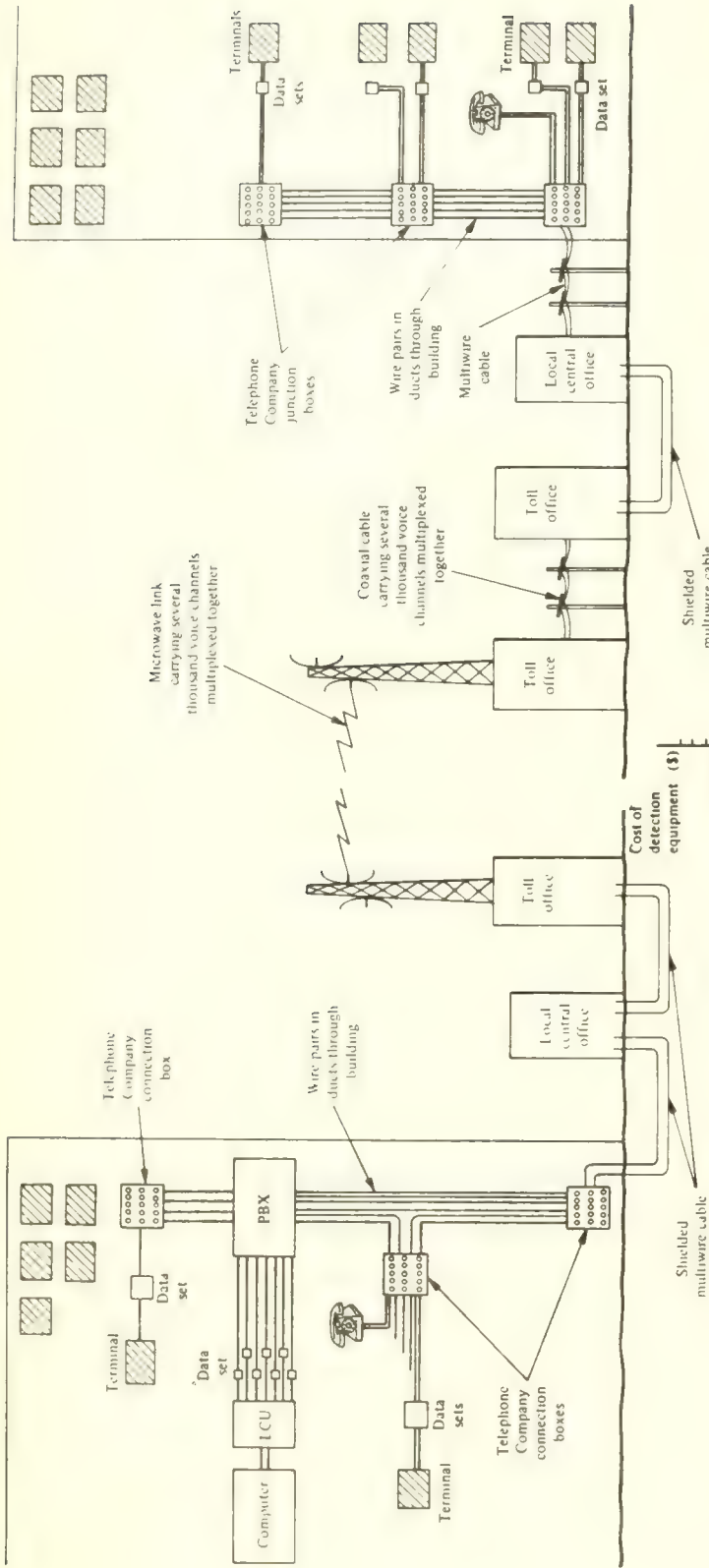
terized information.

Mr. Schneider will discuss methods of intercepting computer data and will recommend means to counter such interceptions.

Mr. Schneider, I believe you have an opening statement.

MR. SCHNEIDER: I do. I trust that every member of the Panel has this hand-out.

[The material referred to follows.]



Jerry Schneider & Company

(213) 883-6700

Source: Security, Accuracy & Privacy in Computer Systems

CHAIRMAN ERICKSON: Yes, we do.

TESTIMONY OF JERRY N. SCHNEIDER, PRESIDENT, JERRY SCHNEIDER & COMPANY

MR. SCHNEIDER: While computers have not quite become a household word, there is no question that over the last 20 years they have become an integral part of the basic functions of American society. From the check-out stand of the supermarket to putting men on the moon, electronic data processing has become an irreplaceable part of our national situation.

In fact, electronic and magnetic data have not only replaced manual bookkeeping and processing and record keeping, but they have also in some respects replaced tangible assets, including money.

For instance, our credit card system would have only been possible on such a large scale today with the use of computers.

And now even moderate and small-sized businesses are turning to some form of electronic data processing which the industry calls EDP.

Accordingly, a survey conducted by Frost & Sullivan last fall indicated that 75,000 firms in the United States are using small business computers, and this does not include the large industrial giants. This figure is expected to grow to 400,000 by 1983.

Moreover, these figures do not include, as I said, the industrial giants.

Clearly, as the number of companies using computer systems grows, so, too, does the abuse of these systems. Although the advantages are efficient and accurate and economical systems, which is readily apparent, the disadvantages are certainly more subtle and undeniably more complex.

Until recently computer manufacturers and users did not pay a great deal of attention to the security aspects or problems inherent in these complex computer systems. In fact, one very important aspect of electronic data processing is that little is really understood in terms of how easy it is to penetrate a computer system and manipulate both employees and outsiders for a variety of reasons, such as gaining competitive information, for fraudulent financial purposes, or by disgruntled employees or anti-establishment activities activists who may want to destroy all or part of the stored data within the computer.

Unfortunately, all too often executives relegate the responsibility of these matters to their normal security departments, which is good as far as it goes, but all too often these individuals are just former law enforcement people and are quite adept in keeping up with physical security in relation to

machines in the computer room and the environment, but they really don't understand some of the highly technical and specialized aspects of protecting data itself, or data interception.

This kind of creates a false sense of security.

Even telephone lines and other electronic methods can be used to circumvent physical security.

Obviously the dangers involved are far from trivial. Given the computer's integral role in most corporations and government offices today, penetration of the computer by the unscrupulous can have a devastating effect on a company's operations, not to mention the functions of government.

More importantly, unlike most crimes against corporations, if the perpetrator is sufficiently sophisticated, it may be months or years before his illicit manipulations are discovered. In fact, there is reason to believe that hundreds of such illicit manipulations are taking place at present. Some of these will eventually be discovered, but others will never be found unless government officials and corporate executives learn about the urgent need for proper precautions.

By now I am sure you are all aware of the massive Equity Funding fraud that occurred in Los Angeles, and similar stories relating to computer rip-offs. But rather than regale you with a series of anecdotes and horror stories, I would like to point out that what makes many of these instances particularly disturbing is that more often than not, although Equity Funding was an exception because a stockbroker tipped off officials on that one, detection of these types of crimes had generally been discovered by accident and not by purposeful methods.

What can businesses and government do to counteract these threats by unscrupulous operatives?

I have come up with a list of 12 suggestions which I would like to introduce at this time, which just touch the tip of the iceberg.

Obviously, an electronic data processing system and each user has problems that require a thorough analysis but as a general guideline these are some ideas that might be considered.

The first point is to limit the number of employees with access to terminals, tapes, and printers to as few as possible.

Two is screen job applicants, keeping in mind the profiles of perpetrators that have been observed from past actions, past cases, previously related computer crimes.

Three: Rotate programmers and other staff so that no one has too much time to successfully commit a crime—and banks are very good at this.

Four: Separate operating and programming functions so that no one person does both.

Five: Change passwords and access codes frequently, especially when there is a high turnover of employees.

Six: Restrict and monitor all attempts to gain access to a system.

Seven: Randomly monitor processing in an open and public way, similar to the technique of using a police cruiser on a patrol. This lets everyone know that work is being done and checked.

Eight: Keep detailed records of time usage that will show if an application suddenly starts to take an unexplainable amount of run time.

Nine: Scramble or possibly use cryptographic techniques to make stored data more difficult to be deciphered by unauthorized people.

And, ten, use specialized guard files and programs with adequate safeguards to make the use of special programs without authorization difficult to obtain.

Eleven: Set up identification code systems to record who uses the system.

Twelve: Screen or investigate the security procedures and operations of vendors that supply time, programs, or equipment.

In response to the desirability and feasibility of legislation broadening 18 U.S. Code 2510 and 2511, I feel these sections should be amended to include specific references to computer terminology such as items of data communications, not including oral communications, items such as baud, which is the rate of speed for transmitting data; modum, which is the device used to connect the telephone line to the computer.

In addition, crimes related to electronic data processing should be spelled out very precisely. As it stands, a perpetrator is free and clear from the law to be able to tap into the data bank of the computer and steal private dossiers on people.

The sections were written long before the concept of computer-related crimes was contemplated, which was 1964—not to mention perpetrated.

As a consequence, it has become imperative that safeguards against such activities be well and accurately defined. Clearly with the advent and acceleration of space age technology, it is not only logical but imperative to bring our legal system up to speed.

At this time what I would like to do is to explain to you—first, are there any questions?

CHAIRMAN ERICKSON: Yes. I will call upon Mr. Hershman to interrogate you on behalf of the staff.

MR. HERSHMAN: Mr. Schneider, you have supplied to us this morning a diagram of computer transmission. I wonder if you might briefly explain to us what this represents.

MR. SCHNEIDER: Yes, Mr. Hershman.

On the top part of the chart—this is what is considered to be a flow chart relating to tracing the logical points in which a data wiretapper would attempt to place a data tap.

As you see on the far left part of the diagram—you see a computer and it goes through the handler, which is the LCU, the data sets. The data sets are the devices that actually connect the computer, itself, to the telephone line. As I mentioned, we call them modums in the industry. And the terminal, itself, is nothing more than a device, just like a typewriter, and they even have portable terminals. You can carry them around in briefcases. And the data set is sometimes placed within a terminal.

I will relate it to possible places where the wires could be tapped so one could receive information relating to the transmission of data from the computer to the user, so that one could manipulate data within the computer, itself; one could access files, so to speak, or at the telephone company junction box, at the PBX level, the wire pairs through the conduits.

One could potentially tap the line, let's say, at the microwave point.

MR. HERSHMAN: Mr. Schneider, if I may just interrupt for a minute. What type of information could be gained by someone wishing to conduct electronic surveillance on data transmission? Could you give us some examples?

MR. SCHNEIDER: All right. Relating to the credit transactions, we have just recently come into a phase where we are now using an incredible amount of credit cards in our society. And the transmission of information, the processing of information, let's say, from what we call the point of sale, which is the merchant—if you go into a restaurant and want to use a credit card—take the case of American Express. If you want to make a transaction, when the system was manual-based, they took the credit card and validated it and figured out how much the charge was and put the draft through.

Well, this is now becoming obsolete. Right now if you will go into a restaurant you will find an electronic terminal that they put the credit card into and it reads the mag stripe on the back of the credit card. I will show it to you. It is this little stripe (indicating). And that is encoded data on the credit card, itself. That is fed into a terminal and it is transmitted by wire to the credit card center where the transaction is immediately processed. That is, they immediately charge you for the meal rather than waiting for the manual paper to clear and use a messenger.

So how can this system be abused and how has it been abused in the past? The system is new so we

don't understand what all the abusive situations are. One can only speculate and guess what would happen unless adequate safeguards are taken to protect us.

For a would-be wiretapper to tap the dedicated pair, which is the line associated from the restaurant to the card center, he could hold up transactions. If he understands the form in terms of the way information is placed into a computer, he can credit his account by \$5,000 as an example. Or he can charge to someone else. He can set up phony account numbers.

There is a consortium of different things one could do.

MR. HERSHMAN: Mr. Schneider, by overhearing computer transmissions could one steal the proprietary trade secrets of a corporation?

MR. SCHNEIDER: As an example, yes. We have systems where you have a computer and there is a lot of different subscribers on the system. People are constantly using the same shared computer. And if one user on the computer has proprietary trade secrets, so to speak, or classified personnel information, it is conceivable that if a person knew the code of the other person, he would be able to go ahead and retrieve the information.

Now, in the case of wiretapping, one could merely place the same modum or data converting device on that line and receive the information.

In the case, let's say, of organized crime—if they were to transact business, that is, bookmaking information, let's say, from one of their field offices to their central computer—and it has been found that organized crime is now using computers—they could transmit data from one point to another.

Now, specifically related to wiretapping, if they wanted to—well, I have kind of got off to another area right now.

MR. HERSHMAN: The point I am trying to make is, as the law is now written, we describe the interception of communications as the aural interception. If you are intercepting transmissions from one computer to another, that wouldn't fall under that particular law, would it?

MR. SCHNEIDER: No.

MR. HERSHMAN: Is this a modern-day method of conducting industrial espionage? Could it be considered that?

MR. SCHNEIDER: I believe it can. The situation is that in terms of aural communication, that is voice communication. And data communication is of a different nature. And it is not specifically written into the law in section 2510.

And in terms of a vehicle with which one could commit espionage, yes, it is.

MR. HERSHMAN: How long would it take to install an eavesdropping device on a computer data transmission system?

MR. SCHNEIDER: Relating to wiretapping a line?

MR. HERSHMAN: Say wiretapping, yes.

MR. SCHNEIDER: Well, the perpetrator would have to get a modum, in other words, a device that is similar to the type that is being used to transmit the data from the computer to the user.

These devices are readily available through any electronics supplier. There are a number of firms that will sell these devices to the general public.

MR. HERSHMAN: Are they expensive?

MR. SCHNEIDER: You can lease one for \$25 a month.

Now, you can take this device, and as our last witness mentioned, if we go to these telephone equipment rooms in a building and there is a data line—and they are clearly marked. They have little red rubber insulators on them and they say "Data Line" on them so a wiretapper knows exactly where to go.

He could set up shop, let's say, right in the building, so to speak, and monitor all the transactions that are occurring between the computer and the user.

MR. HERSHMAN: Mr. Schneider, do you know of any actual cases where electronic surveillance was used to steal computer data?

MR. SCHNEIDER: Specifically, I can only recite cases that involve credit transactions, and these are only newspaper accounts.

MR. HERSHMAN: And these are more for altering the data, though, rather than stealing them; is that correct?

MR. SCHNEIDER: Yes, altering credit files by electronic interception.

MR. HERSHMAN: What is your background in computers, Mr. Schneider?

MR. SCHNEIDER: Specifically relating to computer security, I had set up a consulting business in 1972. And my background is electronic engineering. And I am virtually self-taught and self-educated with relation to working on computer-related crime cases. I have worked with the Stanford Research Institute which did a study for the National Science Foundation on the abuse of computer systems, and I personally investigated approximately one hundred computer-related frauds where I was asked to obtain evidence.

One case I studied was the actual first search warrant to search the memory bank of a computer which was the *People v. Jeff Ward* in Alameda County in 1971.

MR. HERSHAMAN: But in fact your career started out on quite a different foot, didn't it?

MR. SCHNEIDER: Yes, it did.

MR. HERSHMAN: Would you explain to the Commission how?

MR. SCHNEIDER: Are you referring to the activities relating to the telephone company?

MR. HERSHMAN: Yes, I am.

MR. SCHNEIDER: Well, in 1971 I had been charged by the District Attorney in Los Angeles for allegedly tapping into the computerized ordering system of the Pacific Telephone Company and I was charged for a consortium of different types of things, relating to theft of property.

What I had done was, while going to school I had set up a rather intricate scheme to place orders into the computerized ordering system and have actual equipment sent to me throughout the county of Los Angeles.

MR. HERSHMAN: And you did that by telephone; is that correct?

MR. SCHNEIDER: That is correct.

MR. HERSHMAN: Would you explain to us how that worked?

MR. SCHNEIDER: I did this by calling the computer up on the dial and actually entering the proper protocol that the computer understands as being acceptable language or acceptable conversation relating to what the computer knows as being an authorized person to use the system or use the computer. And so the computer saw me as what they call a supply foreman. And what had happened was I had devised a system where I was able to crack the code, so to speak, that enabled me to charge equipment up to other people's accounts. And this equipment was then shipped out.

How it was done specifically was that I had done two things.

One, I had reprogrammed the computer so that the computer would understand that my orders were to be charged to a separate account; and, two, I had placed the orders with the standard touch-tone telephone.

MR. HERSHMAN: How much in orders did you obtain this way? How much monetarily?

MR. SCHNEIDER: Well, there was a whole bunch of different accounts in the newspapers. It was said it was a million dollars. The civil suit that was finally settled last year came to \$214,000.

CHAIRMAN ERICKSON: You obtained this equipment actually?

MR. SCHNEIDER: Yes. I set up very foolishly—I am reluctant to talk about it because I think it was so stupid. But anyway, what I had done was I had obtained the equipment and it was dropped to various supply locations. In other words, if I wanted a switchboard sent to a manhole cover in the middle of the night, I could do that. If I wanted ten

telephone poles sent to a manhole cover in the middle of the night, I could do that.

MR. HERSHMAN: I just have one other question, Mr. Schneider.

I would like to read a paragraph taken from an article taken from *Security Word* magazine in October 1972. The article is entitled "Taps to steal computer data. How feasible?"

"While it might be worthwhile in certain cases of industrial espionage to invest money for talent and equipment to steal the information by tapping, the percentages are against satisfactory or rewarding results because of the time. That is, by the time the tap is accomplished, replayed for experts and machines, and puzzled over until the code is broken, that information would probably no longer have any timely usefulness."

Do you agree with that?

MR. SCHNEIDER: Not at all. I believe if the perpetrator has unlimited resources and the skill, the access, and the knowledge to want something bad enough, he can use a data tap as a sophisticated means to obtain the data.

And you have to look at each case on a case-by-case basis.

MR. HERSHMAN: Thank you.

CHAIRMAN ERICKSON: Proceed, Judge Pierce.

MR. PIERCE: Mr. Schneider, in your statement you said that 18 U.S. Code Sections 2510 and 2511 should be broadened. But your recommendation was not very specific.

Can you tell us specifically what statutory amendments you would recommend to cover the electronic data problems you referred to in your statement?

MR. SCHNEIDER: All right. I think specifically you should put, instead of the word "aural" or "including aural communications" the word "data communications" so that if it were ever challenged, the word "data" is in there and whatever an expert says is data, you have that test.

Items relating to the fact that a terminal is used to receive information so that analogous to a bug, so to speak, one could equate the word "terminal."

This is a tool that might be used to commit a crime.

And I am throwing these out in terms of a definition for the statute. Items such as the rate of data, so to speak, might be included, such as 9600 bits per second, 4800 bits per second. These are standard rates of data that are transmitted from the computer which, for an illegal purpose, I believe—if you are tapping the line, you should make it illegal to receive data at these different rates.

MR. PIERCE: Why are those rates magic?

MR. SCHNEIDER: Those are like the blue box codes, the codes that most industrial organizations use to transmit data from one point to another.

MR. PIERCE: Could the rates change?

MR. SCHNEIDER: Not normally, no. So you are making the law specific to that point.

MR. PIERCE: Anything else?

MR. SCHNEIDER: Possibly the use of a computer system, itself, to—I don't know what the judicial questions raised are, but if you can get the law to read using a computer to tap a line indirectly—in other words, being able to set a computer system up so that it can receive information from another computer for the purpose of stealing valuable media within the victim's computer.

MR. PIERCE: Thank you.

I have no further questions.

CHAIRMAN ERICKSON: Judge Sheintag.

MS. SHIENTAG: Thank you, Mr. Chairman.

Just a few questions, Mr. Schneider.

You are aware, are you not, that this section Judge Pierce is referring to says "wire or oral communication."

Do you regard "wire" as sufficiently broad to include electronic equipment?

MR. SCHNEIDER: Not at all. Wire communication, to me, means a telephone connection, a voice telephone path.

MS. SHIENTAG: It doesn't include electronic?

MR. SCHNEIDER: No, "electronic" is even too broad. "Data communications" is about the best word that you can use.

MS. SHIENTAG: Proceed.

MR. SCHNEIDER: "Data communications" is about the best and most specific word you can use. And if you want to get down to the rate of communication, 9600 or 4800 bits.

MS. SHIENTAG: You are an expert in this field?

MR. SCHNEIDER: Yes.

MS. SHIENTAG: Yesterday we heard testimony from manufacturers of electronic surveillance equipment, amongst them somebody from Bell & Howell. The suggestion was made that these devices be licensed with regular serial numbers. Would you suggest that data going to banks likewise be licensed?

MR. SCHNEIDER: It wouldn't make a difference. You are talking about the would-be perpetrator of the crime being sophisticated in it. And he could have good reason to have a piece of equipment anyway.

If you are talking about a corporation that might be the perpetrator of these crimes against another corporation, in other words, to steal competitive trade secrets, they would have a reason to have the equipment.

MS. SHIENTAG: Let's refer only to the equipment, itself, not to the perpetrator or the method.

MR. SCHNEIDER: I see. I think you are starting another gun control problem.

MS. SHIENTAG: I didn't hear that.

MR. SCHNEIDER: You are starting another gun control problem.

MS. SHIENTAG: In fact, that is what the suggestion was, that it be under ATF of the Treasury Department.

MR. SCHNEIDER: I don't think so because there are too many different types of devices on the market now. And data transmission equipment can be made on a hobbyist level easily.

It is like trying to license a typewriter. I really think it is a kind of nebulous thing, although I think a good strong law that would deter the perpetrator would be more effective.

MS. SHIENTAG: Do you think it might be advisable to put the whole equipment, data equipment field, within an agency such as the Federal Communications System?

MR. SCHNEIDER: Relating to what specific aspect?

MS. SHIENTAG: To the technical aspect of it, in that it transmits data in the same way that television and radio do.

MR. SCHNEIDER: Yes. Well, that is a good idea. The telephone company is certainly getting carried away—

MS. SHIENTAG: I beg your pardon?

MR. SCHNEIDER: The phone company.

MS. SHIENTAG: Yes.

MR. SCHNEIDER: They are getting carried away with what they are doing right now. In other words, they are growing, they are proliferating. They have devices coming out every day which the government, itself, doesn't understand.

I don't think you have to set up an agency but I think you could probably incorporate it within the ranks of the FCC so that they further can regulate specifically data transmission. Because it is such a new area right now. You know, we don't even really understand it, it is so complicated—especially law people. It is even difficult for me to understand a lot of things in data communication.

MS. SHIENTAG: One think that is difficult for me to understand is what was the prosecution that resulted in a conviction against you?

MR. SCHNEIDER: Myself?

MS. SHIENTAG: Yes.

MR. SCHNEIDER: I was given relief under a California exception.

MS. SHIENTAG: Did you plead guilty?

MR. SCHNEIDER: Yes, I did.

MS. SHIENTAG: You were very young at the time?

MR. SCHNEIDER: Yes. So I was given a dismissal.

MS. SHIENTAG: You pleaded guilty and you didn't serve any jail term?

MR. SCHNEIDER: Yes, I did.

MS. SHIENTAG: It was a felony?

MR. SCHNEIDER: It was a felony at the time but was subsequently reduced.

MS. SHIENTAG: But that didn't prevent you from opening a business and engaging in this and advising other firms on the method you learned in such a hard way?

MR. SCHNEIDER: No.

MS. SHIENTAG: Thank you.

CHAIRMAN ERICKSON: Chief Andersen.

CHIEF ANDERSEN: Just one question.

In the detection of data fraud on wire—telephone companies can tell by power drop and so on—do you know of any method to tell, computer to computer, whether it is being tapped? Is the technology available today?

MR. SCHNEIDER: No, it is not. It is a point that should be further discussed here. I have the book here called "Basic Elements of Intelligence," available through the Superintendent of Documents, and the level of technology that our law enforcement people have today to understand the nature of data interception isn't adequate. I think that we need to have more specialized areas in law enforcement and more specialized hardware, machines that can detect data taps.

Right now it is difficult in itself to detect voice taps. Data taps are even that much harder.

So I think we have to be able to at least tool ourselves up to the fact that technology is increasing and it is going to be increasing in the next five years to a point where we are really going to be out of control in terms of understanding how to detect these things.

CHIEF ANDERSEN: I notice most of your 12 points, to me, seem either personnel procedure, security, and have little electronic steps. Is it that the technology is just not there?

MR. SCHNEIDER: I am basing it on a more practical environment. Only 1 per cent of the corporations in this country are even reasonably protected against data taps and data fraud. Specifically those things aren't even done that I mentioned in my points. You really have to look at it as an over-all chain and weakest link, and these are probably some of the weakest links that exist within the business community.

Once you do this, then you can go to a more specialized device, such as the possibility of using cryptographic equipment in transmitting data from one point to another, or even the sophistication changes of data rates.

There are a lot of different devices that I know of on the market that can be used as cryptographic ones to encrypt data.

CHIEF ANDERSEN: Thank you.

CHAIRMAN ERICKSON: Thank you.

Professor Blakey.

PROFESSOR BLAKEY: No questions.

CHAIRMAN ERICKSON: I just have a couple of questions.

In connection with this computer theft, is there any way to determine whether or not a computer has been intercepted or had some of the information stored in the computer put within another computer?

MR. SCHNEIDER: Mr. Erickson, it is very difficult in this business. It is not like Sherlock Holmes going in and uncovering heel marks, so to speak. The would-be perpetrator, so to speak, can in a very sophisticated manner, go into the computer, change around the data, take what he needs and then cover his tracks very quickly.

We are dealing in a very liquid medium.

CHAIRMAN ERICKSON: I understand that. But supposing there were trade secrets within a computer and the means of obtaining this was determined by another company that had the equipment that was necessary to take it from this computer.

Would there be any way to determine that that computer had given up the information?

MR. SCHNEIDER: Yes, there are purposeful methods that we could employ to do that.

In other words, specifically, we might be able to institute a number of, let's say, keys or levels to retrieve this very sensitive information.

In other words, it is like the use of two signatures on a bank check, or possibly putting the program in a vaulted area, so to speak, within the computer memory, so a competitor could not get to it as easily.

CHAIRMAN ERICKSON: I understand that. I am asking you if there is any way, once the material has been stolen from the computer, it would be possible to determine that the theft had occurred. Or would it be difficult to detect that the information had been taken from the computer?

MR. SCHNEIDER: Not normally.

CHAIRMAN ERICKSON: Not normally?

MR. SCHNEIDER: Not normally. It is very difficult to tell. If it is done in a sophisticated manner, no. You can't tell.

CHAIRMAN ERICKSON: You can't tell. That is the point I was getting at. In short, your competitor could have all the information that you had and you wouldn't know it except that your computer was still there and you were continuing to build it up and the theft could go on for years.

MR. SCHNEIDER: Yes.

CHAIRMAN ERICKSON: Without any detection?

MR. SCHNEIDER: Right.

CHAIRMAN ERICKSON: The next question: Is it possible for this computer that would act with the other computer to destroy the information that is on the computer? Could you, with a particular device, cause that computer to lose its effectiveness and have all the information that was within the computer destroyed?

MR. SCHNEIDER: Yes.

CHAIRMAN ERICKSON: You could do that?

MR. SCHNEIDER: Yes, that type of sabotage could be done very easily.

CHAIRMAN ERICKSON: I'm sorry; I didn't hear you.

MR. SCHNEIDER: Yes, that type of sabotage could be done very easily.

CHAIRMAN ERICKSON: So if the proper devices were available, something like the computers utilized by the FBI could be kept from carrying out their function or could have the information that was within the computer destroyed?

MR. SCHNEIDER: Any computer system—down at the local level and up at the national level—our whole country could be paralyzed by tapping into a computer and destroying the data within the computer.

CHAIRMAN ERICKSON: And devices exist to do that?

MR. SCHNEIDER: Yes. I mean they are more lethal than machineguns.

CHAIRMAN ERICKSON: That is all I have.

I think we will take a five-minute—oh, I beg your pardon.

Mr. Schneider, I did want to extend to you the gratitude of the Commission for coming here and giving testimony on a subject that, frankly, is more complex than most of us have occasion to expect. But we appreciate it very much.

I think we should clarify one point.

Judge Shientag asked you about this matter where you were charged with a criminal offense.

California has something akin to the Brooklyn plan and you have no criminal record as a result of this.

MR. SCHNEIDER: No, I don't. That is right.

CHAIRMAN ERICKSON: Thank you very much.

MR. SCHNEIDER: Thank you.

CHAIRMAN ERICKSON: We will recess for five minutes.

[Whereupon, a short recess was taken.]

CHAIRMAN ERICKSON: Ladies and gentlemen, we will reconvene.

Richard Coulter.

[Whereupon, Richard L. Coulter was duly sworn by the Chairman.]

CHAIRMAN ERICKSON: We welcome Mr. Dick Coulter. Mr. Coulter is kind enough to appear here today. We had hoped to have a whole panel of industrial security specialists but the other specialists declined our invitation to testify, and for that reason we are deeply grateful to Mr. Coulter.

Mr. Coulter has worked for 18 years in the industrial security profession. He has had extensive experience in education and law enforcement, emergency preparedness and security. For the past 6 years he has been engaged in maintaining company-wide security in Hewlett-Packard Company in California. He will speak on industrial espionage and the need for special legislation in this area.

Mr. Coulter, I believe you have an opening statement?

TESTIMONY OF RICHARD L. COULTER, CORPORATE SECURITY DIRECTOR, HEWLETT-PACKARD COMPANY, PALO ALTO, CALIFORNIA

MR. COULTER: Yes, I do, Mr. Chairman.

Mr. Chairman, distinguished members of the Commission, ladies and gentlemen:

I sincerely appreciate the opportunity to be here today and participate in this portion of your study and review, specifically, the need for legislation to provide criminal penalties as a means of deterring industrial espionage, and to examine the rationale for licensing requirements of individuals and firms who are in the business of providing countermeasure services on a contract basis.

As a matter of definition, my colleagues on the West Coast and I look at industrial espionage in terms of being a possibility rather than a threat. By that I mean the basic approach for industrial security planning in all hazards, including industrial espionage, is to determine the possibility and then design the necessary countermeasures for adequate safeguards.

Does the possibility for industrial espionage exist? I believe it does, even though the number of reported cases have been few. Assuming, then, that the theft of information such as research and development plans, new product design, marketing strategies, production schedules, and so forth, is a possibility, what can business and industry do to cope with the problem?

Most large industrial firms employ full time professional security practitioners—many of whom have the expertise of conducting an in-depth electronic and physical countermeasure sweep. In most cases, these professionals are capable of extending

their contribution in safeguarding sensitive information by participating in the identification of what is sensitive, following with safeguarding methods and conducting countermeasure sweeps.

For those industrial organizations whose full-time security personnel do not have this capability, or the smaller firms that do not have security personnel on the staff, the alternative is to hire an individual or organization on contract to provide this service. However, this is not as simple as it sounds. There are stumbling blocks that exist.

First, the employer is faced with the reality of hiring an outsider to do a very sensitive, internal job. Then, when he attempts to verify the ability, ethics, and reputation of the outsider firm, he finds that no license is required to perform this specific type of service, and any former employers' names are not easily available because of the need to keep that information confidential. The thought then comes to mind, "What if I'm hiring someone to do the countermeasure work that a competitor has on a string to bug me?"

The result? In my opinion, firms without their own capabilities for conducting adequate countermeasure sweeps are reluctant to employ the services of an outsider that can't be checked on. Many believe that existing laws are inadequate to offer protection from the unscrupulous technician. Therefore, the small firm is on its own—and I seriously doubt that an accidental discovery of an electronic eavesdropping device would be reported, partly because of the publicity that might follow, and partly because of the unawareness as to whether the discovery was truly an act of industrial espionage or simply the neglect of a serviceman to collect all equipment and wires after a routine job.

We are all certainly aware that in recent years there has been a tremendous increase in the interest of the individual's right to privacy. That right should not exclude the privacy of those individuals in the business sphere. In my opinion, their thoughts, conversations, private discussions, and business information require the same protection as any other individual.

Without stringent legislation to control the manufacture and distribution of wiretapping and electronic eavesdropping devices, coupled with intelligent licensing requirements for those who offer the countermeasure service for a fee, the possibility of such invasion of privacy may truly become a threat. The end result could very well mean the business life or death of an individual or firm, or at least a serious hazard to growth and security.

Again, I thank you for this opportunity.

CHAIRMAN ERICKSON: Thank you, sir.
Mr. Hershman.

MR. HERSHMAN: Thank you, Mr. Coulter. I am particularly indebted to you for being here today. As the Chairman mentioned, we had hoped to have a panel of experts testify about industrial espionage today. The Commission, in April, did a study and found that a number of major corporations in the country had been victims of electronic surveillance. Unfortunately, in doing the study we had to guarantee anonymity to some of these firms, and when we asked them to appear, they refused. They feel that it might be embarrassing for them to testify about being victims of electronic surveillance.

Some of the results of this study that we did—and the study was conducted amongst members of the American Society for Industrial Security, an organization of which you are a member are as follows: Out of a total of 104 of the individuals, corporate security directors, we contacted, 40 per cent which were involved in the manufacturing business indicated that they were fairly worried about being victims of electronic surveillance.

Forty-nine per cent of the research institutions felt the same way.

Twenty per cent of the sales and service organizations and 54 per cent of the government contractors had some degree of worry about being victims of electronic surveillance.

In addition, 10 per cent of those we surveyed have indicated they were victims of electronic surveillance.

So, Mr. Coulter, I think this is a very, very severe problem today and again I want to thank you for being here.

Could you tell us, sir, what it might mean to your particular company if, in fact, someone engaged in industrial espionage through the use of electronic surveillance and stole some proprietary information.

MR. COULTER: First, Mr. Hershman, I am here representing myself with 32 years in the combined business of law enforcement and industrial security, not as a representative of the Hewlett-Packard Company or its principals.

We have knowledge that there are a considerable number of professional security practitioners, as I mentioned in my opening statement, that routinely inspect their own facilities prior to sensitive discussions or the outlining of newly-designed products.

The Hewlett-Packard Company, I will say, has never to our knowledge in its history had any inkling or there has never been any proof or even so much as a suspicion based on our own capabilities of being attacked under this type of system. The ones that I am familiar with have been publicly announced, starting back into the mid-Sixties with the Botts Dots incident in Redwood City.

It is a fact that there are people who are performing this service on a contractual basis to a lot of large and medium-sized and small companies that cannot either afford these professional security people that have this expertise—these are the people; not my company as such, but speaking as a security individual—these are the companies that I feel need the assistance, some form of protection, from the unscrupulous technician that I previously mentioned.

MR. HERSHMAN: To what extent do you go, sir, to make sure you don't become a victim of electronic surveillance invasion?

MR. COULTER: Are you interested in my discussion about my own company? Is that what you are getting at? What do I do for my company?

MR. HERSHMAN: If you can talk about it?

MR. COULTER: Well, in most countermeasure work, as you well know, Mr. Hershman, it is not something that is openly discussed.

Suffice it to say that we assure ourselves that we are not subjected to electronic eavesdropping by anybody.

MR. HERSHMAN: And you are aware, though, of other companies who have been victims of electronic surveillance?

MR. COULTER: The ones that have been announced publicly, yes.

MR. HERSHMAN: Do you know of any practitioners who are considered experts at industrial espionage per se?

MR. COULTER: I have knowledge of people who profess to have this expertise. These are people from all over the country. They cross state lines to perform this countermeasure work.

The word "industrial espionage" goes a lot further than just the electronic eavesdropping and wiretapping.

CHAIRMAN ERICKSON: Off the record.

[Discussion off the record.]

MR. COULTER: The business of industrial espionage goes a lot further than the electronic eavesdropping and the wiretapping. It goes into the method of identification of what is sensitive and how to protect it, whether or not it is put into computers or whether it is filed like engineering notes; duplicates are kept in a remote storage facility.

So we are looking more or less, as I see it, related to the Commission's interest in what I might have to say, into the ability to eavesdrop on private discussions in board rooms, the office of the president of some company, or perhaps his home.

And when I mentioned the need to curtail the manufacture and distribution of this equipment, it just so happens very timely that we had, before I left to come here, which was yesterday—I received a package in the mail that was dated June 23, which was Monday, and mailed in San Jose, openly, unsolicited, to my company, "Attention: Security Department," and they are listing here a dozen or so devices which include pictures of the wristwatch, Dick Tracy type microphones, the pocket pen.

In the State of California, Section 635 of the California Penal Code expressly prohibits this kind of literature.

I haven't had time to get in touch with the District Attorney, but I will on my return.

MR. HERSHMAN: Mr. Chairman, I wonder if we might not have that entered into the record, or a copy of that entered into the record.

CHAIRMAN ERICKSON: Would you be willing to allow our reporter to cause this to be copied and then return it to you?

MR. COULTER: I have no objections. The people who sent it to me might object, but I have no objections.

[The material referred to follows.]

Dear Sir:

Three security problems, three answers. Our production program extends from a simple alarm device to the most elaborated surveillance system. If you have a security problem, we try to help you. Here are some of our products listed:

Telephone transmitters and devices *

Telephone scramblers

Electronic-optical devices

Directional microphones

Receiving devices

Radio telephone devices *

Camouflaged transmitter *

Mini tape recorders

Alarm devices

Laser alarm systems

Infrared cameras and monitors

Infrared night observing devices

Infrared detection devices

Miniature infrared noctovisor

Briefcase cassette recorders

We construct special instruments to your ideas and needs.

PAMO ASS. INC. a division of PK electronic-Germany.

Governments all over the world trust in PK products.

* No installation from us available.

PROBLEM:

An object or a distance should be controlled invisibly

SOLUTION:

Laser alarm equipment PK 720. With PK 720 distances of 1-15 metres can be controlled. This equipment can be used without any installation work being necessary. If the invisible laser beam is crossed the device will release a signal through the built-in alarm keying system. Single objects can be protected also as the laser is adjustable. At mains failure the built-in battery ensures an undisturbed 100 hour operating time.

TECHNICAL DETAILS:

Dimensions: 220-105-65 mm. Weight 4 kg. Power supply 110/220 V. Additional: Key switch for "on/off" control meter, socket for external power supply adjustment of alarm period, adjustment of distance, socket for external alarm device i.e. siren, horn, light.

Pamo Ass. Inc.

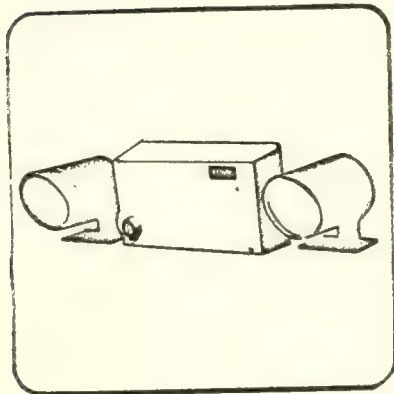
Micro Electr. Security Devices

Sales — Service — Installation

Box 234

Cupertino, Calif. 95014

(408) 244-5247



PROBLEM:

Invisible supervision of an airport open field etc. with an electronic system has to be carried out.

SOLUTION:

Laser alarm system PK 715. This system comprises a transmitter a receiver and a control unit. The system is available in different executions for 250-6500 metres. The transmitter transmits a modulated signal. The receiver will decode this message electronically. If the security line is passed by persons the receiver will not receive a signal anymore and this will cause an alarm device to sound.

TECHNICAL DETAILS:

Housing metal splash-proof. Power supply 12-15 V. 110-220 V. Output: 10 A. floating. Temp. range -30 C. to +60 C.

PROBLEM:

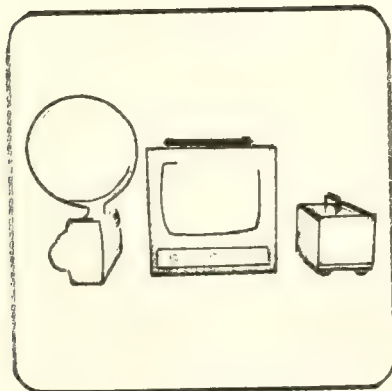
During the night you require a device for supervision of buildings, car parks, entrances etc. which can be controlled with a monitor.

SOLUTION:

Infrared TV camera and monitor PK 310. With this system an inconspicuous TV supervision in complete darkness is possible. This system is mainly used by the police, customs and companies for supervision of factories.

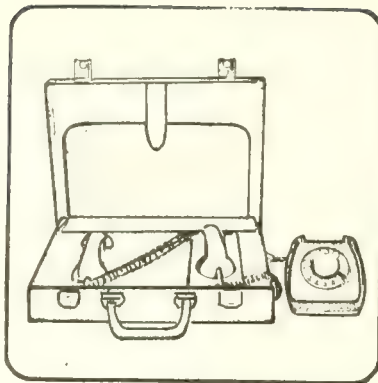
TECHNICAL DETAILS:

Infrared searchlight: Dimensions: Diameter 100-210 mm. Weight: 1100 grams. Power supply 110/220 V. Power 100 W. Range: 500 metres.
Infrared camera: Dimensions: 50-130-270 mm. Weight: 2500 grams. Power supply 110/220 V. Valve: Vidicon
Monitor: Dimensions: 270-270-230 mm. Weight: 5500 grams. Power supply: 110/220 V. Valve: Diameter = 23 cm.



Pamo Ass. Inc.

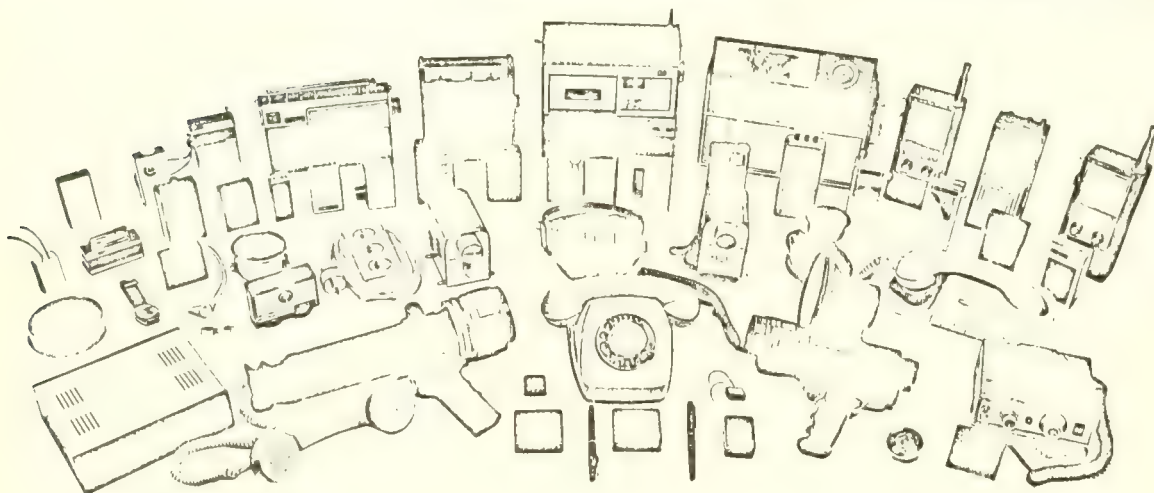
Micro Electr. Security Devices
Sales — Service — Installation
Box 234
Cupertino, Calif. 95014
(408) 244-5247



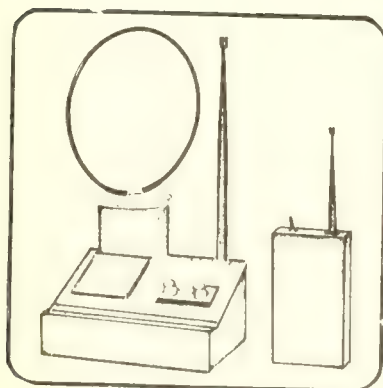
Telephone Scrambler



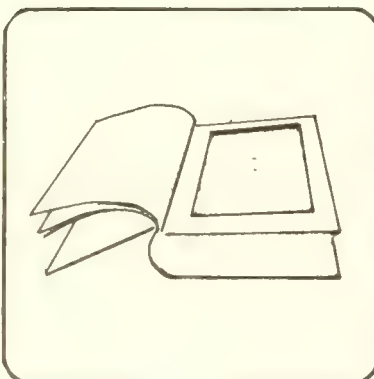
Alarm System Do it yourself



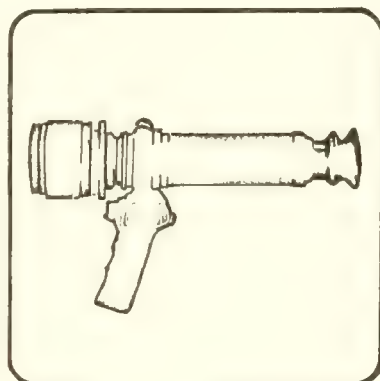
Some of our production line



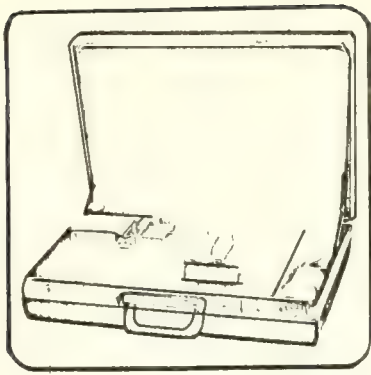
Vehicle tracing system



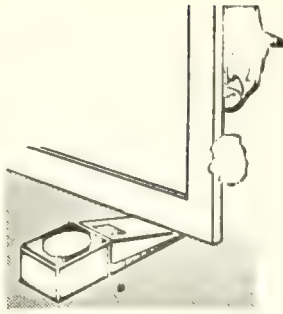
Tape recorder in a book



Intensifier by remaining light (passiv noctoviser)



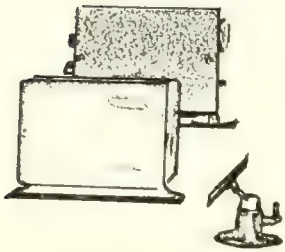
Psycho stressmeter PK 925



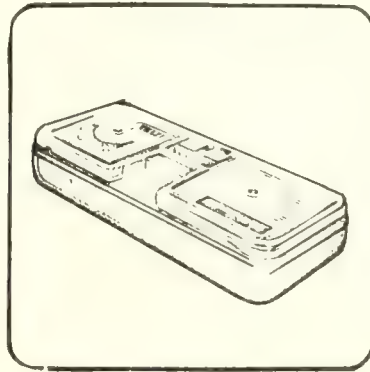
Bloc-Alarm



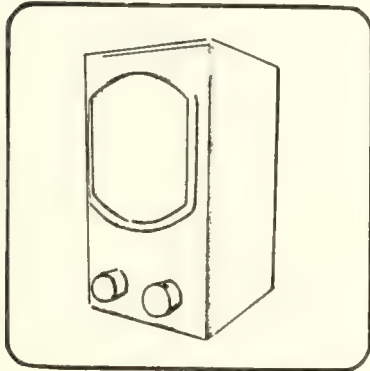
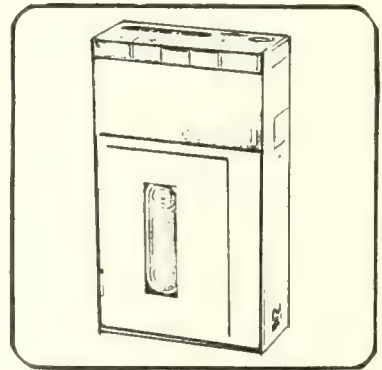
Microphones



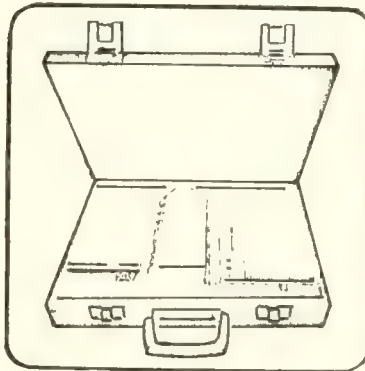
Infrared Alarm System
for Homes Cabins etc.



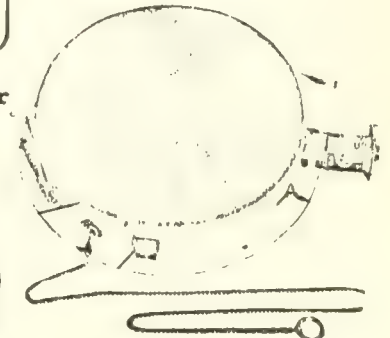
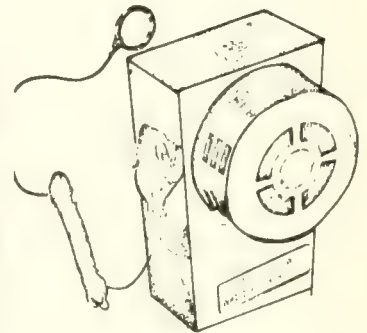
Mini Tape Recorders



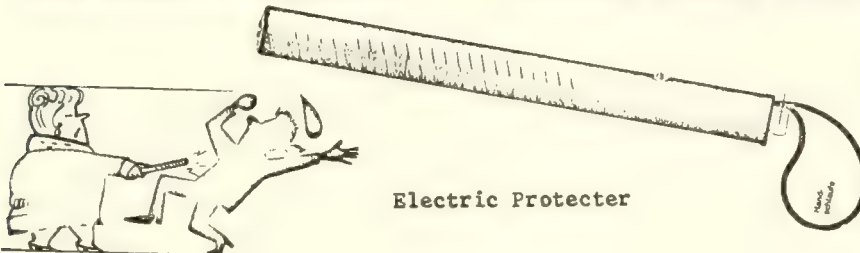
Alarm System with Acustomatic



Briefcase Cassette Recorder



Burglar and Fire Alarm



Electric Protector

MR. HERSHMAN: This came to you unsolicited?

MR. COULTER: Yes.

MR. HERSHMAN: Do you often get advertisements for electronic surveillance devices through the mail?

MR. COULTER: It stopped for about a year and a half, but it has started up again. And an interesting note on this thing is I have personally reviewed it because it is a Post Office box in a small town called Cupertino, California, and the telephone number didn't register as being in that community. So, through friends, it turned out it is an apartment house in another location in California.

MR. HERSHMAN: What is your normal procedure when you receive something of this nature?

MR. COULTER: I am in communication with most the of the law enforcement people in northern California.

MR. HERSHMAN: Have any prosecutions resulted from such information turned over to them by you?

MR. COULTER: This is the first one that has actually come to me unsolicited since Section 635 was put into the book.

MR. HERSHMAN: But under federal law, this would seem also to be a violation.

MR. COULTER: Well, I am responsible to report findings that I have either to the Palo Alto police department or the Santa Clara County District Attorney's office, which I do in each and every case. It is their determination to make whether they pursue it or not.

MR. HERSHMAN: Have you ever had opportunity, Mr. Coulter, to engage the services of an outside countermeasure technician?

MR. COULTER: I haven't because I have done that work myself. Prior to coming to this company I was in that business, along with investigations and contract articles. And I did countermeasure work for other large companies.

MR. HERSHMAN: You have a strong feeling that people engaging in these services should be licensed; is that correct?

MR. COULTER: I believe that the people that are performing this service on a contract basis should be licensed so that the people who need their services would have some place to be able to check. Right now there is none. There is no licensing requirement for that specific type of work in the State of California. And if Joe Small that operates a business such as the ones that have been publicly noted that they have been subjected to that crime—they have no place to turn. Because they cannot turn to the people who are in large industry,

we don't have the time. Our attention and our contributions are devoted to our own company.

But the people who are in the smaller companies, in my estimation, need some sort of protection, and the only protection I consider valid would be the licensing of these people through an intelligent system of examination to determine their knowledge of the equipment, and their complete awareness of federal and state laws.

This is not limited to one state. There is one person I know that has this capability and is ethical and has an excellent reputation. But he travels all the states in the United States or abroad. And other than just a basic investigator's license, I believe this subject is so technical and so sensitive that these people need some form of protection that they can make sure that this individual is licensed.

MR. HERSHMAN: Mr. Coulter, do you find that large industries are spending more and more money as part of their security budget for devices which will counter electronic surveillance?

MR. COULTER: Some companies are.

MR. HERSHMAN: So then they do perceive the threat to be very real; is that correct?

MR. COULTER: Well, as I mentioned, there is quite a difference between threat and possibility. Somebody has to tell you or make some kind of a formal statement to you that they are going to do something before it actually carries the connotation of a threat.

We think it is possible. We say anything is possible. But until such time as somebody calls one of my colleagues and says "We are thinking about performing an act of industrial espionage at your facility," I don't really consider it a threat.

MR. HERSHMAN: What would your procedure be if you did discover a device?

MR. COULTER: Well, my procedure would be to immediately inform the cognizant law enforcement agencies of this, as it is a violation of several of the California statutes. And we would proceed from there with the assistance of the District Attorney's office, under Section 499(c) of the California Penal Code, which is one of the more recent ones.

CHAIRMAN ERICKSON: Would you mind keeping your voice up.

MR. COULTER: Maybe it would help if I switch microphones.

Is this better?

CHAIRMAN ERICKSON: Much better.

MR. COULTER: Section 499(c) of the California Penal Code specifically prohibits the acts of industrial espionage and the theft of trade secrets in the State of California.

However, that doesn't deter people, because the penalties are not that severe, unless you get caught

for the exact same violation of the same section more than once.

And the others, on the eavesdropping devices—that is Section 632—wiretapping, eavesdropping, and the manufacture, sale, and possession, all carry for the first conviction in the State of California \$25,000 or one year in the county jail.

So, looking on the other side of the fence for a moment, if somebody says “Would you bug Joe Small’s office here; I want some information. He is coming up with a better fence than I can build,” the fear of being fined \$25,000 if I am going to charge \$50,000 for this doesn’t have much of an impact on me.

But I still think—and one of my reasons for being here is to speak in behalf of the security industry—a lot of people in the business—not necessarily my own company—fear that we are subjected to people who can provide the so-called countermeasure work. And possibly under that guise, the person that is on the string of many companies purposely to plant devices.

It was rumored before I came here—I tried to confirm it—I have heard one small company in Sunnyvale actually found a device that was planted by the man who found it.

That is the type of action I think that somewhere along the line the general public or business needs help on.

I would like to recommend, before I leave, that the Commission consider the staff developing, through association or contact with people who are in this business or profession, a model statute that would cover these things a little more specifically than some of the state laws now provide.

MR. HERSHMAN: Mr. Coulter, some of the companies with whom we spoke indicated that if they found a device they wouldn’t report it because it would be an embarrassment to the firm.

Would you comment on that?

MR. COULTER: I think so. Nobody likes to believe that they would be the subject of an attack. By the same token, you find a lot of people who are attacked in their homes or on the streets who have the same fear of adverse publicity. And particularly the people in the more or less 100 per cent commercial market—I would assume that these people would consider that some of their prestige might be damaged if it was widely known and publicized that they had been victimized. All I can do is assume that is why they wouldn’t report it.

And the other part is because they are not aware. There are not too many people who, if they took the receiver apart on the handset on their telephone and something fell out of it—I fully believe a lot of people might pick it up and actually

throw it away. They haven’t caught up with the world being spooked, being scared by that kind of activity. You can’t really expect a lot of these people to live their every-day lives and perform their every-day business with that kind of a fear attitude.

So they don’t expect it and if they do find it, they don’t realize what it is.

MR. HERSHMAN: Thank you, Mr. Coulter.

CHAIRMAN ERICKSON: Judge Pierce.

MR. PIERCE: Mr. Coulter, you mentioned in your statement that there should be intelligent licensing requirements for those who offer countermeasure services for a fee.

Specifically what licensing requirements would you recommend?

MR. COULTER: Judge, I just happen to have some notes here.

MR. PIERCE: Good, I am glad I asked that question.

MR. COULTER: I have broken it down into two sections. I think the basic requirement should be, number one, that the individual who is going to perform the service have a criminal-free background; and, two, that he be bonded; and that he provide a minimum of 3,000 hours of experience and certification.

The second part of it is there should be an examination to provide thorough knowledge of both federal and state laws he is going to operate in relating to industrial espionage, wiretapping, and electronic eavesdropping.

Part of that examination should be examples of countermeasure equipment knowledge, rather than the man that comes to your door with a little black book and says, “I do countermeasure work.” It is a very impressive thing. He opens his big box and most people wouldn’t know whether it is an RF detector or a box of cigarettes in a little black box.

The other part of the examination, in my estimation, should be the facets of structural physical examination. Because equally as important as the countermeasure work for the use of electronic detection equipment for implanted devices is the thorough physical examination. And I believe that the operator or the person who is performing this service should have full knowledge of the equipment and how to do the job in order to be licensed to do it.

MR. PIERCE: You mentioned 3,000 hours of training. Was that it?

MR. COULTER: Yes.

MR. PIERCE: Where would you get that training?

MR. COULTER: Well, in many cases people who are now performing this type of service on a contract basis to large industry are former agents of

various agencies of the United States Government, where it was a necessity to perform that type of service in several areas of the world.

MR. PIERCE: Well, assume a person does not work for the government at any time in his career, how would he get the experience then? Working for a company that does this? Or how?

MR. COULTER: Well, he would probably set himself up as a trainee working with some company, and the physical examination portion of it is a very simple matter of thoroughly searching, taking things apart, tracking one end of a wire, for example, to the other, being able to feel and see.

During the course of his early employment he would be so instructed by a thoroughly licensed individual on the use of electronic equipment.

MR. PIERCE: Does your company train its own staff in countermeasure services?

MR. COULTER: No, I am the one in the company that has this capability.

MR. PIERCE: You are the only one in the company that has this capability?

MR. COULTER: Yes.

MR. PIERCE: Thank you. No further questions.

CHAIRMAN ERICKSON: Judge Shientag.

MS. SHIENTAG: Mr. Coulter, what does Hewlett-Packard manufacture?

MR. COULTER: The Hewlett-Packard Company manufactures electronic, measuring, scientific, medical instruments.

MS. SHIENTAG: Does it do anything with data banks?

MR. COULTER: Data banks?

MS. SHIENTAG: Yes.

MR. COULTER: Manufacture of computers?

MS. SHIENTAG: Computers.

MR. COULTER: Yes.

MS. SHIENTAG: Are there any recommendations that you have with regard to that area of your corporate work, to insure there is no espionage in that area?

MR. COULTER: Well, I find it difficult to believe that too many large business people would put very sensitive information into a computer. Most of the sensitive information during the course of research and development is kept in engineering notes. It is usually highly safeguarded by the engineer who is doing the development itself.

As they progress through the stages of development and they get into the building of prototypes and things like this, the documentation on it is usually very, very restricted, and it is treated much in the same vein as classified information would be.

MS. SHIENTAG: If you were selling something that was not as sensitive as electronic material—if you were selling, for example, shirts in a store—you

could have a store Dick watch what was going on and prevent any theft of the merchandise that you have.

Do you feel because you are dealing in highly secretive matters you are at a disadvantage in comparison with a retail store, for example?

MR. COULTER: Oh, definitely so. I would imagine there are quite a few people that would like to have the inner-most thinking of a company such as mine.

MS. SHIENTAG: Yes.

As I read the law, I don't find any way that you can protect yourself without engaging in some countermeasures that in themselves might be illegal.

Do you have any comment on that?

MR. COULTER: I don't understand what you mean.

MS. SHIENTAG: Well, if you see a bug, you can lift it up—you can take a telephone receiver and see if there is a telephonic transmitter there. But if you want to sweep the place, you might have to use detection material for which you have no warrant, as not being properly authorized by the federal law now.

MR. COULTER: I'm sorry, but the detection equipment and physical examination to examine on your own facilities—

MS. SHIENTAG: Well, you wouldn't buy the equipment which you introduced in the form of a letter from a California firm. You wouldn't buy that kind of equipment would you, in order to protect yourself?

MR. COULTER: No. That was not to protect us in any way, shape, or form. There would be no need for us to purchase eavesdropping materials.

MS. SHIENTAG: But if you were to purchase it, that, itself, would be a violation?

MR. COULTER: Yes. That is the reason I cited that as an example, a very recent example, by those people sending it to me.

MS. SHIENTAG: Yet you have the capability of manufacturing equivalent material to detect a violation?

MR. COULTER: We don't manufacture that. We manufacture hand-held calculators and computers and field survey equipment and scientific equipment.

MS. SHIENTAG: Then how do you actually detect the industrial espionage, any violation of your secrecy?

MR. COULTER: Well, we have not detected any theft of our trade secrets. We do not feel that we have been subjected to the theft of an industrial espionage act. One way that we can assure ourselves that nobody is attempting to obtain informa-

tion from us is through the use of electronic detection equipment. We could examine any areas where there are going to be sensitive discussions held.

MS. SHIENTAG: Where do you get this electronic detection equipment? That is my question.

MR. COULTER: It is available through licensed firms anywhere—not almost anywhere, but there are several large national firms that manufacture detection equipment.

MS. SHIENTAG: It was my understanding that it was only available to the police authorities in certain areas.

MR. COULTER: Not the countermeasure equipment, no. The positive, as they call it, or the equipment used to amplify or transmit voice communications—that is restricted and we are not supposed to be able to buy that, although according to the gentleman who is offering it for sale we can.

But I have no personal knowledge of any laws controlling my buying an RF detector or a telephone analyzer to assure that the telephone has not been tampered with.

MS. SHIENTAG: So you do use such equipment?

MR. COULTER: I have used such equipment.

MS. SHIENTAG: Thank you very much.

MR. HERSHMAN: I would like to say that this afternoon we will have some of the manufacturers of the countermeasure equipment appearing before us and they will demonstrate and display some of their equipment.

CHAIRMAN ERICKSON: Professor Blakey.

PROFESSOR BLAKEY: Mr. Coulter, your resume indicates you have been in the law enforcement field for approximately 32 years, 18 of which you have been in the industrial security profession; is that correct?

MR. COULTER: Yes.

PROFESSOR BLAKEY: And I notice that your recommendation is for the licensing not of private detectives as such, but rather of security people doing countermeasure work; is that correct?

MR. COULTER: It is anyone who offers to provide this service on a contract basis for a fee, including private detectives.

PROFESSOR BLAKEY: Do I understand one source of your recommendations to be skepticism of the ethics and ability of people who are presently in the field?

MR. COULTER: I couldn't really cite anybody that I would have that type of suspicion of. Again, it is a possibility.

PROFESSOR BLAKEY: You are a member of associations of other people in the security field, aren't you?

MR. COULTER: Yes.

PROFESSOR BLAKEY: I take it you have had conversations with other security people?

MR. COULTER: Yes.

PROFESSOR BLAKEY: Do I understand your testimony to be that some of the people who offer this debugging service are really charlatans?

MR. COULTER: All are not members of our Society. All do not advertise in the professional trade publications. It is done by letter form and oftentimes by a personal visit.

PROFESSOR BLAKEY: Is it your judgment that a number of these people are selling a service for which there is not as much need as they would lead their customers to believe?

MR. COULTER: That is also very true. I know of no one that I've checked with just before coming here, and I have talked to quite a few of my colleagues and none of us have ever found anything.

PROFESSOR BLAKEY: I want to get this very clear in the record.

It is your judgment, based on your experience and the associations you have had with other people in the security area, that the danger of industrial espionage is larger in the newspapers than it is in the board rooms?

MR. COULTER: I think it is, yes, sir.

PROFESSOR BLAKEY: And that part of the reason for this is that people who are selling this service have an economic interest in creating the need by scare tactics?

MR. COULTER: Very much so. And also I believe that people, when they are in the, quote, "board rooms," are a little more concerned today on safeguarding their own information than they were several years ago.

I think the ability to extract trade secrets, let's say, either through electronic eavesdropping or any other method is less of a concern today than it is from the absent-minded type individual who might relay this information, something he is working on, at the local saloon.

PROFESSOR BLAKEY: And your suggested remedy or at least partial remedy for this problem is licensing and regulation of certain facets of the security field; is that correct?

MR. COULTER: Yes.

PROFESSOR BLAKEY: Thank you, sir.

CHAIRMAN ERICKSON: Chief Andersen.

CHIEF ANDERSEN: I have no questions.

CHAIRMAN ERICKSON: Mr. Coulter, just a few questions.

We all know that there is all but a national paranoia about the fear that you are being heard when you talk over the telephone, or that there is electronic surveillance.

This may be partially a product of Watergate.

As a result of that, your job for Hewlett-Packard is to assure your employers that they are not being

made the subject of this industrial espionage, and it is protective maintenance in effect?

MR. COULTER: Yes.

CHAIRMAN ERICKSON: Now, when you get into this area there are many devices, of course, and to know what these are you have to go through considerable training to recognize the various means. You can't look for something without knowing what it is; isn't that right?

MR. COULTER: That is right; yes, sir.

CHAIRMAN ERICKSON: And how it operates?

MR. COULTER: Right.

CHAIRMAN ERICKSON: So what your recommendation is is that these people that hold themselves out as experts in this area of countermeasures, if you will, should have to demonstrate their ability so the public will be safeguarded against the man that comes to the door and says, "Do you have any reason to believe that you are being wire-tapped?" or "Do you know whether you are or not?" and the man says, "I would certainly like to know." And he says, "I can tell you for \$5" and maybe goes in and waves a magic wand around and maybe finds something he has brought himself.

MR. COULTER: Yes.

CHAIRMAN ERICKSON: It is to provide public safeguards against the charlatan.

MR. COULTER: Right.

CHAIRMAN ERICKSON: The restrictions that you put in the proposed license or the requirements for the license, I would have to say are a little more stringent than they appear to be in most states for, say, private investigators.

MR. COULTER: They are.

CHAIRMAN ERICKSON: And they are considerably more stringent than they are for some of the professions.

And the imposition you have made upon the licensing would limit it to those who have had extended training.

Now, is there a place available to get that type of training except the college of hard knocks and by going through police academies?

MR. COULTER: Most of the training is available, to my knowledge, either through the manufacturers of the devices—some of the companies that manufacture the detection equipment also provide in-depth training.

As I mentioned earlier—

CHAIRMAN ERICKSON: Of course, those companies wouldn't give the training to anyone who wasn't a prospective market for that product?

MR. COULTER: No. They would be looking for them to use their detection equipment if they trained them.

CHAIRMAN ERICKSON: So the person that would then want to get in the field and get the training couldn't get it anywhere through any formal education?

MR. COULTER: It would be a situation where people who already have—there are a considerable number of people who have either retired or resigned from the military services and the various agencies that have been doing this type of work for years. And they are making themselves available now. And it is very possible that in the future we might see, if this continues to be such a scare to the general public, schools being set up to train people in this type of work.

I know of only one law enforcement agency in all of northern California that has this capability, and it is primarily due to one individual—a lieutenant in the department. He feels that this should be part of the service that his department could afford to people who cannot find someone that they would feel comfortable with.

CHAIRMAN ERICKSON: Of the major companies that you have come in contact with—and, of course, the size of Hewlett-Packard and the work they do is known to most of us—in connection with that, have you come to know what the number of experts in your field is that are employed by major companies such as, say, Ford; such as General Motors? All of them have someone who would have a similar position to that which you occupy.

MR. COULTER: In most large companies the security manager has the capability of performing this type of service.

CHAIRMAN ERICKSON: This Society you belong to holds annual meetings, I assume, and at that time determines what the developments are in the art?

MR. COULTER: Yes.

CHAIRMAN ERICKSON: From your experience, apart from these news articles that you have read, do you know of any industrial espionage that has actually occurred?

MR. COULTER: No, only those that have been made public. The people that I have talked to who do this routinely, and still do it routinely, have not found anything in their sweeps. They have not been able to detect the loss of any so-called trade secrets.

CHAIRMAN ERICKSON: Theft from their computers.

MR. COULTER: No.

CHAIRMAN ERICKSON: When you say 'the ones that have been made public,' I believe you gave examples and I am afraid I did miss the examples that you gave.

MR. COULTER: I started off in Redwood City with one of the first ones, Botts Dots, which has been indicated in several publications. People have written about it. This is the incident where one company had developed a reflectorized type dot, if you will, to go on the white line on the highway. And the president and vice president of another company had attached a suction-cup type device leading directly to the tape recorder which was in the bushes.

And when the incident was over they felt they had all the information necessary and they sent the man back because they wanted to recover the device—they said the device cost them \$300 or something like that. And that is when they were actually caught, when they went back to recover the device.

That was the first one that I was aware of.

CHAIRMAN ERICKSON: How many years ago was that?

MR. COULTER: It was in the mid-sixties—I forget the exact year.

And the incidents are very seldom made public if they are found.

I believe that the people that I know and have worked with all these years—if they actually found something, they would actually pass this information along to me. But according to our conversations, we haven't found any.

CHAIRMAN ERICKSON: Of course, electronic surveillance through wiretapping could be something that occurs outside of the premises that you have searched?

MR. COULTER: Oh, yes.

CHAIRMAN ERICKSON: So, as far as the physical facilities, you haven't found anything within those facilities that you are aware of?

MR. COULTER: Right.

CHAIRMAN ERICKSON: Do you feel that apart from the suggestions that have been made there is adequate protection for industry in this particular piece of legislation known as Title III, the Omnibus Crime Control and Safe Streets Act?

MR. COULTER: Well, I think it is a step in the right direction. I think more emphasis could be placed on all facets.

I would agree with my predecessor here that the ability to obtain information once you are able to figure out the codes as they enter into the computers is getting to be a point of concern among a lot of people. And more and more people are becoming educated in the ways to obtain codes.

Of course, if the codes are changed frequently enough, this continues to make it more difficult for these people.

But it could, under the broad umbrella of industrial espionage, include thefts of electronic data and information.

So I find nothing that my predecessor at the table had to say in his recommendations that I wouldn't also be in agreement with. It should include them.

And looking further down into it, the people who have the ability to be mobile, move from one company to another, for example, I can do my work for the XYZ Company and am asked to go to the ABC Company and work for them at the same time and, because of your talents and expertise, one would find it an easy way to commit industrial espionage to do it that way because then you are sure you are getting what you really want and you don't have to wait for somebody to activate their electronic eavesdropping device.

CHAIRMAN ERICKSON: Mr. Coulter, we very much appreciate your coming, and particularly for the detailed and provocative suggestions you have made that will be considered by the Commission, and will appear within our report.

Thank you very much.

At this point in the record we will insert exhibits 9, 10, 11 and 12 which were submitted for the record.

[The exhibits referred to follow.]

EXHIBIT NO. 9

INDUSTRIAL ESPIONAGE

In the spring of 1975, the National Wiretap Commission queried a number of corporate security officials concerning the effect of electronic surveillance laws have had on industrial espionage. Has the Law (18 U.S.C. 2511-12) been effective in curbing the use of illegal electronic surveillance against the nation's businesses? Do corporate security officials feel able to cope with the dangers of electronic espionage? Should firms dealing in countermeasure services and/or equipment be licensed?

With the aid of the American Society for Industrial Security, three hundred seventy-two officials were consulted, and one hundred four of them chose to participate in the survey. These one hundred four broke down into the following categories: 46 manufacturers, 23 research and development organizations, 20 sales and service organizations, 11 government contractors, and 4 miscellaneous businesses.

The questions asked and the total results were as follows: Questions 1 and 2 involved identifying the type of firm and size. Question 3. Do you believe that there has been less industrial/business espionage by means of electronic surveillance since the passage of the 1968 Federal Wiretap Law?

24 Yes

32 No

48 Don't know

Question 4. How worried are you about eavesdropping and the possible invasion of your firm's privacy?

10 Very worried

31 Fairly worried

51 Not too worried

12 Not at all worried

Question 5. Do you believe your organization has ever been the subject of privacy invasion through electronic surveillance?

- 15 Yes
- 79 No
- 10 Don't know

Question 6. If Yes, by what method?*

- 13 Telephone interceptions
- 8 Audio room interceptions
- 0 Video surveillance
- 1 Other—Government mail

Question 7. Type of device used?

- 5 Radio frequency
- 6 Hard wire
- 8 Don't know
- 1 Other—phone slug, bumper beeper

Question 8. Authority notified?

- 1 Federal
- 0 State
- 1 Local
- 6 Telephone company
- 1 Other—Private investigator
- 8 None

Question 9. Was an investigation of this invasion successfully pursued by your organization or a government authority?

- 3 Yes
- 11 No
- 2 No answer

Question 10. If No, why not?*

Question 11. Do you believe that your organization can combat electronic surveillance through modern countermeasure techniques?

- 76 Yes
- 20 No
- 8 To some degree/don't know/no answer

Question 12. Do you have in-house expertise for countermeasure activities?

- 46 Yes
- 58 No

Question 13. Have you had occasion to obtain countermeasure services from a private firm or individual?

- 31 Yes
- 71 No
- 1 No answer
- 1 Now considering this step

Question 14. Were you satisfied with the quality of those services?

- 24 Yes
- 6 No
- 73 No answer
- 1 Don't know

Question 15. Would you recommend licensing for those engaged in countermeasure services?

- 82 Yes
- 18 No
- 4 No answer

*16 persons responded to Questions 6 through 10; 15 had answered Yes and 1 had answered Don't know to Question 5.

**Answers to Question 10 are included in the following tables.

FINDINGS AND CONCLUSIONS

The results of this survey reveal that a substantial number of the consulted organizations are highly concerned about the possibility of electronic surveillance of their activities. Out of a total of one hundred four, thirty-one described themselves as "fairly worried" and ten were "very worried" about this possibility. Those concerned comprise almost 40 percent of the manufacturers, 49 percent of the research institutions, 20 percent of the sales and service organizations and 54 percent of the government contractors who participated in the survey. Forty-four percent of the organizations maintained in-house expertise for countermeasure activities, and almost 30 percent have hired private firms or individuals to provide countermeasure services. However, one fourth of the respondents do not believe their organization could successfully combat a privacy invasion. The fact that 40 percent of the respondents chose not to identify themselves presents another indication of uneasiness among the participants. Those who remained anonymous were more than 1.5 times as likely to be very or fairly worried about the problem than were those who identified themselves.

In addition to the high level of concern among almost half of the respondents, 16 of them reported actual incidents, or suspected incidents, of electronic surveillance of their companies. Thirteen of these privacy invasions involved telephone interceptions, and eight involved audio room interceptions. Five respondents indicated that both methods had been employed. Once the problem surfaced, the victims of electronic surveillance were generally reluctant to notify any authority other than the telephone company. Although four discovered the privacy invasion well after it had occurred so that investigation was not deemed worthwhile, of the remaining twelve, six notified the telephone company, and one also notified local authorities. A seventh respondent notified federal authorities, and an eighth notified a private investigator and is currently considering taking additional measures. The other four took no steps whatsoever.

Finally, the respondent's concern and uneasiness regarding problems of electronic surveillance is reflected in their replies to the more general questions posed by the questionnaire. Almost half of them feel uncertain about the effect of the 1968 Federal Wiretap Law on the incidence of industrial espionage, and 30 percent believe the Law has had no effect whatsoever. Of the officials who participated, an overwhelming majority, about 80 percent, recommended licensing of those engaged in providing countermeasure services.

ANALYSIS OF SURVEY RESULTS

Question 1

The consulted officials were given the option of not identifying the name of their organizations, although all were asked to describe the type and size of their firms. The following chart represents the numbers, for each type of business, of respondents who gave and failed to give the names of their organizations. Only two respondents failed to identify the type of firm involved; these were placed in the 'Miscellaneous' category.

Type of Organization	# Identified	# Anonymous	Total
Manufacturers	25	21	46
Research and Development Organizations	14	9	23
Sales and Service Organizations	15	5	20
Government Contractors	6	5	11
Miscellaneous	2	2	4
Totals.....	62	42	104

Question 3

Respondents	Yes	No	Don't Know
46 Manufacturers	8	15	23
23 Research and Development Organizations	8	5	10
20 Sales and Service Organizations...	7	5	8
11 Government Contractors.....	0	5	6
4 Miscellaneous	1	2	1
104 Total.....	24	32	48

Question 4

Respondents	Very worried	Fairly worried	Not too worried	Not at all worried
46 Manufacturers	4	14	21	7
23 Research and Development Organizations	3	9	9	2
20 Sales and Service Organizations	1	3	13	3
11 Government Contractors.....	2	4	5	0
4 Miscellaneous	0	1	3	0
104 Total.....	10	31	51	12

Respondents	Very worried	Fairly worried	Not too worried	Not at all worried
62 Identified.....	4	15	35	8
42 Anonymous	6	16	16	4

Question 4 – Additional Correlations

Respondents	Question #	Yes	No	Other
10 Very worried...	3	0	6	4 Don't know.
	5	3	5	2 Don't know.
	11	8	1	1 To some degree/Don't know.
	12	7	3	
	13	4	6	
	14	3	1	6 Not applicable.
31 Fairly worried..	3	9	11	11 Don't know.
	5	8	17	6 Don't know.
	11	22	8	1 No answer.
	12	13	18	
	13	10	20	1 Now considering this step.
	14	6	3	1 No answer. 21 Not applicable.

Respondents	Question #	Yes	No	Other
51 Not too worried.	3	12	11	11 Don't know.
	5	2	47	2 Don't know.
	11	29	11	5 To some degree/Don't know. 1 No answer.
	12	21	34	2 No answer.
	13	15	34	2 No answer.
	14	13	1	1 No answer. 36 Not applicable.

12 Not at all worried.	3	3	2	7 Don't know.
	5	2	10	
	11	11	1	
	12	6	1	
	13	2	9	1 Not applicable.
	14	1	1	10 Not applicable.

Question 5

Respondents	Yes	No	Don't know
46 Manufacturers	5	35	6
23 Research and Development Organizations.	0	20	3
20 Sales and Service Organizations.....	5	14	1
11 Government Contractors.....	4	7	0
4 Miscellaneous	1	3	0

Of 15 who answered "Yes" to Question 5:

7 notified no authority whatsoever.

6 notified the telephone company, one of whom also notified local authorities.

1 notified a private investigator and is currently considering other measures.

1 notified federal authorities.

Of 7 who did not notify any authority:

2 discovered the invasion several years after it had occurred.

2 handled the problem internally, 1 out of fear of publicity

1 responded "disappeared"—presumably either the suspected invasion or the need for investigation disappeared.

1 indicated that there was suspicion of an invasion only, without proof.

1 gave no answer at all.

Of 10 who answered "Don't know" to Question 5:

1 indicated that there was some evidence, although not conclusive, upon which his/her suspicion was based.

9 gave no further details of their suspicions.

Respondents	Yes	No	Don't know
62 Identified.....	3	54	5
42 Anonymous	12	25	5

Question 10

Respondents	Responses, (Comments)
5 Manufacturers.....	Device discovered several years after it had been placed in operation. There was no hope of any resolution. Incident occurred prior to 1965. Equipment removed whenever found. Do not want publicity. Believe government agency initiated wiretap. Current—a few days before this writing—investigation not completed. No answer. (Did not notify any authority. To Question 5 indicated positive belief of a privacy invasion but without proof.)
1 Research and Development Organization.	Discovered the possibility too late to investigate.
5 Sales and Service Organizations.	No definite proof of electronic surveillance. Found out about it years later. Little cooperation, if any. (Notified the phone company.) Not applicable. (Investigation was successful.) Not applicable. (Investigation was successful.)

4 Government Contractors	Decision to conduct countermeasures pending. Results were not conclusive. Not applicable. (Investigation was successful.) No answer. (Did not notify any authority.)
1 Miscellaneous	Disappeared.

Question 15

Respondents	Yes	No	No answer/Don't know
46 Manufacturers	33	11	2
23 Research and Development Organizations.	21	1	1
20 Sales and Service Organizations	15	5	0
11 Government Contractors.....	10	0	1
4 Miscellaneous	3	1	0
Totals.....	82	18	4

TAPS TO STEAL COMPUTER DATA: HOW FEASIBLE?

What are the microwave links, the dedicated land lines, and the ordinary telephone lines giving to the computer data thief? Are these transmission vehicles providing easy access to all of our corporate secrets?

Because computer access on shared time arrangements is frequently obtained by dedicated land lines or by means of telephone lines, a great deal has been written lately about the possibilities of computer pilferage through tapping either of these phone lines enroute, or placing taps on egress lines leaving the company offices for the underground cable. In addition, awed sounds are being made about the possibilities of compromising computers through a microwave tap.

SECURITY WORLD went out looking for some computer experts, and asked them some pointed questions about the real security problems involved in potential tapping of all kinds. As a result, in the following article, various kinds of taps are defined and their possible percentages of danger are evaluated.

TELEPHONE TAPS

A standard telephone tap is understood by security officer and layman alike. Whether that tap is planned for a regular telephone line or on a dedicated land line, the electronics and procedures for tapping would be the same. The protection instituted to safeguard the computer transmission against such a tap would have to be the same as that instituted to protect a normal voice—though there is greater danger of losing accuracy in transmission with computer data.

However, it is probable that scrambling is not really necessary in the case of computer data transmission if it goes out as encoded information. Several factors actually mitigate in favor of the privacy of such a transmission. First, the computer transmission is digital, not analog, as is the voice. Second, it is structured according to the program of the system into which the information is being fed, and from which the information is coming.

In order to decode such information, that is, to make

the information usable to anyone tapping the lines to steal the transmitted sounds, a great deal of expensive talent and equipment would be required. Finding the proper lines would itself be an enormous task once the transmission had gone onto multiplex cable. Beyond that, it would take time—and the use of talent and equipment cited above—to break the code.

While it might be worthwhile in certain cases of industrial espionage to invest the money for talent, and equipment to steal the information by tapping, the percentages are against satisfactory or rewarding results because of time. That is, by the time the tap is accomplished, replayed for experts and machines, and puzzled over until the code is broken, that information would probably no longer have any timely usefulness.

The very real problem mentioned above of finding the proper transmission when tapping into telephone lines or dedicated land lines should also be considered a factor in favor of security. Literally hundreds and even thousands of transmissions are carried over any one given cable at one time. Clearly the problem of isolating the stream of sound needed to complete the tap would be at best challenging.

A MICROWAVE LINK

In certain instances, something called a microwave link is used in the telephone transmission system. It can be described as "just another way of running a wire, except that it doesn't happen to be a physical wire."

What happens is that the material carried on the telephone lines up to the point where the microwave link begins is then transmitted by waves through the atmosphere across a particular area and picked up at the scheduled reception point (where the microwave link ends) to be put back on the telephone line and continued on its way.

continued on page 46

WHAT ABOUT DATA TAPS?

continued from page 45

If, for example, the telephone lines are being run through mountainous country, it is much easier to send from peak to peak than to lay lines overland. A small transmission station may be built on one knoll, and another station built 40 miles away on another knoll. Each would have two small antennas that point at each other and be able to send messages directly across the gap instead of running down and around over hundreds of miles of land area all rough and rugged and difficult to properly lay the cable.

The beam of transmission for microwave is fairly narrow. However, it is possible to actually set up equipment a half-mile away and pick up enough of the stray energy to record what is happening. Again, of course, such a pick-up would be a terribly expensive proposition; and, again, once the data is acquired it still has to be turned into something usable.

Further, setting up equipment complex enough to complete the total theft operation might be difficult to do undetected. But it is possible to set up a small installation to record the microwave information so that the thief can take it somewhere else to work on it. Such a tapping would use video recording to put the microwave on the tape.

The microwave link can be thought of as nothing more than a two-way television transmitter, and we would be talking about picking up the voice (audio) portion only if we were tapping a microwave link. Microwave transmissions can only be accomplished on a line-of-sight basis. There is no infiltration of alien transmissions from unexpected geographic areas such as occur with an AM radio.

HOW DOES WAVE TRANSMISSION WORK?

Consider a radio wave, which you can think of as pure tone, at a million cycles per second. (Compare this mentally with a high frequency note on the piano which may be ten thousand cycles per second in order to get a clear idea of what we are talking about.) The frequency is a million cycles, then, compared to the ten thousand cycles of a high piano note.

Next, the wave is electronic. It is a wave on which you can impose something called modulation. If it is amplitude modulation, that means the person transmitting can make the amplitude of the modulation bigger or smaller at the rate of the information he wants to transmit. For amplitude modulation, then, you have a basic wave frequency and you have superimposed information on that wave in modulated, overriding waves of controllable amplitudes. Remember the amplitudes are made bigger or smaller depending on the amount of information that has to be transmitted.

Within a small range, it is also possible to change the frequency of the carrier wave (or band). This is called frequency modulation. If instead of a million cycles per second you make it just a few cycles below or a few cycles above, you can change back and forth. This gives additional flexibility.

Now, if you accomplish this preparation of the carrier wave and the overriding modulation in microwave, it is possible to transmit it with a very small antenna and also focus it in a tight little beam, so that with relatively low

power you can get good quality transmission to another precise point.

As a matter of fact, the precision is so great that if you are just a few degrees off target the beam won't be received at all. That is one of its advantages; the transmitter can focus directly on the target instead of wasting a lot of energy splashing the transmitting information all over the side of the mountain! This type of transmission has been analogized as "focusing the sunlight to burn out the lieutenant." The convenience factor of using this method is great. That is the reason for overlaying modulation on carrier to transmit over space on what is called a microwave link.

TAPPING MICROWAVE LINKS

First of all, it is necessary to have a receiving antenna on your secret interception that will pick up a microwave out of the air. From there on you have a choice.

Your first option is to record it undetected. If this is done, you have not demodulated the information that you have imprinted on the magnetic video tape. You have not removed the carrier in order to isolate the modulation. You have merely recorded directly all that has been transmitted. Typically, that takes a higher level of recording capacity because a microwave is very high frequency.

Another alternative is to attempt to have some detection circuits in the equipment, and then record the detected material rather than the total transmission. There would be less of a problem in the recording process, but it is also very likely that you would lose some information as you were tapping because the detection method may not be exactly the same as the modulation method used in transmission.

What we are really saying is that some recordings that try to detect before they record may encounter modulation that is hard to untangle and therefore miss some of the data. There are ways of modulating so that it makes it difficult for somebody who doesn't know exactly what your techniques are.

There is nothing magic about the microwave link. It is certainly harder to tap into than a telephone line in that it is probably more expensive to do so. On the other side, it may be a bit easier to do the tapping undetected. Also, microwave links typically carry thousands of channels. So the problem immediately becomes one of which channel is the one you want, and how do you isolate it?

SUMMARY

Certainly theft of information by tapping either telephone lines or microwave links is technically possible. However, despite all-too-rampant scare comments about such taps as a large threat to the security of computer information, the security officer should take more careful stock. Considering the time-factor, the complexity and the cost, there is every reason to feel that, if such a tap were executed, the stakes would have to be so high as to be perhaps at the level of separate governments, and the financial resources on a par.

Perhaps one day these elaborate taps will be a proper concern to the security officer. In the opinion of those we talked with, however, the time for concern at this level is not now.

SECURITY WORLD wishes to add a word of thanks to Mr. John Cosgrove (whose article appears on page 14 of this issue). To assist us in bringing to our readers the widest feasible spread of information in this special Computer Edition of our electronics and communications issue, he has freely and generously given of his time as a reviewer. Particular attention was given to articles authored from composite interviews and research, which appear without bylines or interview credits.—ED.

*For the sake of simplicity, no effort is made to go beyond an example that illustrates the point; all details and/or technical possibilities are not included.

SECRETS FOR SALE

Industrial Spying: \$6 Billion Drain on U.S. Business

BY AL MARTINEZ

Times Staff Writer

A laser beam fired from an unmarked van stabs through the closed window of a building across the street and picks up conversations in a secret meeting.

An answering service operator taps into a telephone line and a man in an inconspicuous motel room listens to private talks between two electronics experts.

A beauty operator asks seemingly casual questions about the kind of work her customer's husband (a chemist) does and sells the intelligence to a buyer whose identity she may never know.

Code names, secret drops, infiltration, minicameras, spies, counter-spies, telephone bugs, blackmail, double agents, radio transmitters an eighth the size of a penny, parabolic microphones—the instruments and elements of espionage.

But it's the kind of espionage that has nothing to do with military or diplomatic secrets.

The information sought is commercial secrets—ranging from chemical formulas worth millions to customer lists, from product designs to fashion designs, from manufacturing techniques to transportation routes.

Both amateur and professional agents steal an estimated \$6 billion a year in ideas, information and materials from American businesses and industries, and the practice is becoming more widespread.

The figure may even exceed \$6 billion, one investigator says, "because like rape, a lot of cases go unreported."

In the majority of instances, the spy if caught isn't prosecuted. You can't put a man in jail for selling ideas, and to prosecute for stealing

secrets a company would have to prove that the information is a secret in the first place—and you can only do that by revealing the secret.

Industrial Research magazine estimates there are hundreds, possibly thousands, of industrial espionage agents operating in the United States today.

They are often employees or ex-employees of the victimized firms. The amateurs will work in groups, the professional works alone. Their motives can be revenge or money or both. Their income ranges from a

Please Turn to Page 23, Col. 1

few hundred dollars a job to a \$100,000 yearly income.

Many professional spies are former policemen gone astray or unscrupulous private investigators. Some amateurs are homosexuals blackmailed into espionage to protect their reputations.

Their victims are companies that produce toys, automobiles, fuel, electronic devices, drugs and chemicals, aircraft and flight components, fashion wear and cosmetics.

Organizations have gone bankrupt when trade secrets were stolen by industrial espionage agents. One Los Angeles firm lost half a million dollars in sales in 90 days because of a stolen secret.

California and New York are especially vulnerable to commercial espionage—probably because of their vast industrial output, the great number of firms involved and the intense competition between them.

But they are also becoming more aware of the problem, and companies specializing in antiespionage are introducing a whole new range of sophisticated gadgetry into the fight against spying.

The George Wackenhut Corp. of Florida, third lar-

gest industrial security organization in the nation, has seen its business double in four years to an annual revenue of \$100 million—an increase it traces directly to a new demand for antiespionage work.

Sometimes just plain honesty will trap a spy. It did last year in Chicago in what is considered to be the largest industrial espionage case in U.S. history.

Two men tried to sell trade secrets of the Monsanto Chemical Co. valued at \$500 million. They offered them to the Stauffer Chemical Co. for \$5,000—and were turned in.

In another case, a former employee of Procter and Gamble tried to sell the company's sales promotion program and complete marketing for Crest toothpaste — which was valued at \$1 million—to Colgate-Palmolive for \$20,000.

Colgate cooperated with the thief just long enough for him to be arrested by the FBI in an airport men's room.

Not every case ends that way. A pesticide company employee quit after a violent argument. He took with him the secret of a successful pesticide formula and a customer list and handed them over to his new employer — the first company's competitor.

That wasn't enough for him, however. He went back to his first employer and altered that formula to render the product ineffectual. By the time the company discovered the change in the formula, its business had disappeared and it eventually went bankrupt.

While employees and former employees constitute a good part of the industrial spy business, there is also

a cadre of professionals who know their work well.

They will often infiltrate a company for the specific purpose of stealing its secrets. If an agent can't get a job there, he may pose as a customer, a buyer, a salesman, a freelance writer or even a fire inspector.

He will bring with him an assortment of miniature bugging devices—one that spikes into a wall to tap the conversations on the other side, one that fits into a pencil left casually on a desk, and a great number that work on telephones.

If he is a high-priced professional spy he might even utilize a \$22,000 laser gun microphone. He fires the beam through a window to pick up conversations 300 yards away.

Other spies have learned to tap computers and steal data stored in their information banks. But more often than not, they can discover what they want to know by just picking up used ribbons from electric typewriters, and by taking used carbon papers and crumpled notes from waste baskets.

Who hires the professionals? Occasionally a firm that just plain wants its competitor's secrets. But also, according to a Los Angeles private investigator specializing in anti-industrial espionage, it's a company that doesn't know that what it is doing is illegal.

Milo Speriglio, director of Nick Harris Detectives, gets two or three telephone calls a day from businessmen or industrialists wanting his firm to engage in espionage.

"It's incredible," he says. "They look upon it as just another form of marketing research. I tell them that it's espionage and I won't do it.

"Last week, if you can imagine, we got a call

from a funeral home to do undercover work in a mortuary."

Almost every company would like to know what its competitor is doing, Speriglio says.

"They figure spying might be borderline but that it's no big deal. Their logic is that other businesses are probably doing it to them, so they should do it too.

"When they ask us to spy and we turn them down, they almost invariably say, 'All right, then who do we call?'"

Speriglio estimates that of those businessmen or industrialists who read this story, more than a hundred are unknowing victims of spies—either their phones or firms are bugged, or espionage agents have infiltrated their companies.

Even detective agencies are not immune from being spied upon, he adds. A competitor tried to plant a spy in his firm. The man was trapped by a polygraph test given to all prospective employees and admitted what he was trying to do. Speriglio turned his name over to state licensing authorities.

"A good espionage agent is limited only by his imagination," Speriglio points out—and most of the pros are quite imaginative. "A clever one can find out anything he wants to know."

The person who becomes a spy, he says, is looking for quick money and has no scruples. He is, on an average, about 25, white, single, without a criminal record, has had about a year of college and is accustomed to earning about \$8,000 a year.

Usually, he is highly transient—moving in and out of an area fast when his work is done. He often gets into spying through association with other spies, and stays at it no longer than a year.

The average spy earns* from \$500 to \$750 a week for a job that usually lasts three months. But the pay can go higher, depending on the stakes. Speriglio knows of one who got \$25,000 for a single effort.

"Industrial spying," he says, "is one of the easiest crimes to commit. The spy is rarely caught and seldom prosecuted."

What is important about Speriglio's job is stopping the spy in the first place. That simple, yet complicated, act can save his client from being swept out of business.

A company may notice that its sales are suddenly sagging or that it is being consistently underbid or that its secrets are popping up in products manufactured by a competitor. They call on Speriglio.

He begins by checking on all the company's employees. He might place an undercover agent in the plant, thereby discovering who has access to what information, where it is discussed and where it is typed or otherwise recorded.

False information is fed out to discover leaks, and suspects are carefully followed to determine their contacts.

Telephones and rooms are debugged. In one build-Speriglio discovered 17 bugs—all of them on different frequencies. He sweeps his own office for listening devices once a week thoroughly.

In another instance, Speriglio discovered a tapped phone and a spy's effort to discover what a firm was going to bid on a high-paying contract.

He had his client feed false information over the phone (a bid considerably higher than it actually was), thereby frustrating the espionage and, eventually, catching the spy.

A former San Francisco private detective who asked to go unnamed admits that he used an illegal wire tap to check on an employe suspected of being an industrial spy and cleared him.

This same detective, aware that another client's phone was being tapped, traced the culprits to an unexpected source — the FBI.

Speriglio says that what really would inhibit spying in the first place is preemployment screening: the use of polygraphs and background checks on prospective employes.

Deputy Dist. Atty. Philip Halpin, a member of the major frauds division for two years, believes that another way to cut down on the growing problem of industrial espionage is to create new laws.

Presently, there is only one statute in California which covers the theft of trade secrets—499C of the state Penal Code.

"I rejected more cases than I prosecuted," Halpin says, "because they fell short of 499C. There's only a small body of law on industrial espionage. It's a new, unsettled area."

About the most a victimized company can do now is file civil suit in an effort to prevent a suspect firm from using the stolen secret for at least 18 months — usually long enough for the victimized company to cash in on profits gleaned from the secret.

In some cases, the plaintiff may even recover damages. In other cases, the legal action is dropped after the year and a half.

Industrial espionage is becoming more commonplace, Halpin guesses, because of the current profit squeeze, fiercer competition from inside and outside the United States, and

soaring labor and production costs.

Others speculate that the biggest stimulus to espionage has been the tremendous growth in research and development and the progress in technology. They hold out lures of big money to be made on something as small as a scientific formula.

One of the growing methods of espionage is reverse engineering. Products obtained legally (by lease or purchase) or illegally (by burglary, for instance) are simply disassembled by competing firms to determine what is in them and how they are put together.

Unless the product is obtained illegally, reverse engineering itself is legal. Which is one good reason, Halpin suggests, why it has become so popular.

"In these cases, industrial espionage isn't as exotic as it sounds. It just involves an engineer in a back room who's an expert at what he's doing."

It is mostly the amateurs, says Halpin, who engage in cloak and dagger operations.

"Some guy sees a movie and gets real Mickey Mouse about what he's doing. He'll have drop points, code names, the whole bit.

"The pro just goes about his business all alone, realizing that the more people who know what he's doing the more chance he has of getting caught."

Occasionally, a spy hired by one firm to steal another company's ideas will turn into a double agent—working for both sides at the same time.

"It goes even further than that once in awhile," Halpin says. "He'll steal a secret for one company and decide he can make more money peddling it himself.

"He might put it up for bid or just sell the same information four or five times to all the competitors. Or maybe, if it's an entire product he's stolen, he'll sell it piecemeal."

A spokesman for the Wackenhut Corporation predicts that the problem of industrial espionage will continue to grow—which will increase the profits of his and other organizations involved in antiespionage.

"On the business side," he adds, "I suppose that's good. But one regrets the necessity to profit from such an abuse of morality."

Security: Industry's fears grow

Eavesdropping

rises in plants

and board rooms

By ADRIAN PERACCHIO

Staff Writer

Scene: the carpeted, wood-paneled boardroom of a large corporation in Manhattan. A private detective in shirtsleeves passes his hands quickly and lightly under the polished wood of the conference table. He crouches near floor vents, takes them apart, and peers in them. He stretched up to acoustical tiles, removes them, and pats the openings. He touches and plucks gingerly a transmitter the size of his fingernail.

Cut to: a large stock brokerage office in northern New Jersey. A supervisor partly hidden by a frosted glass divider reaches toward a bank of winking lights on his telephone console. He taps a button and begins to listen to a phone conversation between one of his brokers across a large room and a client. Neither the broker nor the client are aware they are being monitored.

Cut to: Kennedy Airport. The loading warehouse of an international airline. Closed-circuit TV cameras peer down from various angles, scanning every move cargo loaders make, panning silently in overlapping arcs 24 hours a day.

The three scenes are repeated with increasing frequency in private business and industry, where concern for security is growing to levels bordering on the obsessive.

Much of the concern appears to be justified by increases in employee pilfering, hijackings, and even pirating of trade secrets.

But as the need for tighter security grows more pressing, it begins to clash with the jealously guarded concept of an individual's right to privacy. This clash has already produced lawsuits.

Some lengths to which corporate executives go to make sure competitors don't gain an edge are motivated by a touch of trendy paranoia bred by the Watergate wiretapping episode, some investigators say. Nevertheless, a vast security industry is growing in the wake of all these fears.

"Businessmen are developing gradually a greater awareness of security," says Robert Hair, assistant professor at the John Jay College of Criminal Justice. Hair chaired a four-day seminar on corporate security in New York City last week,

sponsored by the American Management Association.

"A look at the growth of the private security industry is proof positive," he said. "Some 35 years ago private security lagged far behind public or governmental security. Today private security is just about as large."

With Watergate bringing home the use of electronic eavesdropping and monitoring of conversations in politics and government, businessmen realized their phones could be tapped, for example, with astonishing ease, and they began to take measures to prevent that possibility.

Electronic eavesdropping by anyone except a law enforcement officer carrying a court order, is illegal. It has been against the law ever since 1968, when the federal Omnibus Crime Control and Safe Streets Act was passed.

Its illegality, however, does not prevent mail-order electronic houses

that roughly one in 100 bug sweeps results in anything being found.

vate industry can only be guessed at.

\$500 for a room

A month ago, Pinkerton's Inc., the oldest private investigating agency in the country, announced formation of a new division, called Executive Electronic Countermeasure Service—in other words, debugging.

For an unspecified fee, electronics experts employed by Pinkerton's "sweep" offices, boardrooms, or whatever a client demands in search of hidden bugs, using homing devices to smoke them out.

"We've been doing it for years," said Henry C. Neville, vice-president of Pinkerton's, "but the demand has become substantial enough for us to have formed a separate division."

Pinkerton's officials declined to say how many searches they perform, and how many of them actually turn up bugs. But McCrie said

Sweeping for bugs is not cheap. Most investigators charge about \$500 to clear a room. "And for that, most agencies will only do a very, very small room," McCrie said. Office suites cost considerably more.

Some investigators look upon bug sweeps with a skeptical, if not jaundiced, eye. They say that in some cases, searching for bugs can be akin to a doctor giving a placebo to a hypochondriac patient, an expensive way to soothe ruffled corporate nerves.

"Hell, I know a guy who, when he's a little hard up for money, actually plants a bug when he doesn't find one in his sweeps," a Newark private investigator said. "The guy who hired him gets really uptight then, and more than likely will call him back once a month before the monthly

from doing a brisk business in the sale of listening and recording devices whose minute size and ease of concealment can only qualify them as bugs.

"The law hasn't tested this field yet, so there is a lively sale of eavesdropping devices," said Robert McCrie, editor and publisher of Security Letter, a biweekly newsletter on corporate security distributed in 26 countries.

Private investigators are flooded each week with leaflets and order forms from mail-order companies offering sophisticated eavesdropping devices, often with a warning that some states prohibit their sale.

A debugging service

Because of its nature and its illegality, the extent of bugging in pri-

meeting to check the room out again."

In at least one case, being the target of a bug was a sign of corporate status in a New York corporation. An electronics expert in northern New Jersey said an up-and-coming executive hired him to plant a bug in his own office.

Playing one-upmanship

The executive then would complain to management that something was wrong with his phone. The in-house security force would then check his phone and find a bug.

"See, what this man was doing was playing, a one-upmanship sort of game. You know, if my office is bugged by the competitors and yours isn't, then I'm more important than you are."

Nevertheless, serious bugging is definitely going on, though the public only finds out about it when cases finally come to court. In the majority of cases, neither the victim nor the culprit is eager to dis-

close the extent of the illegal activities—a matter of poor image for both.

When wiretapping cases do come to court, they often involve employees who are suing their employers for having infringed upon their privacy.

Macy's employees in San Francisco filed a \$13 million damage suit against their company on a wiretapping charge earlier this year. Macy's said it was done as a way to prevent shoplifting, and the judge ruled in Macy's favor, but a civil damage suit is still on.

"What came out of that case is that wiretapping of employees is a very common practice," said Robert Smith, an American Civil Liberties Union lawyer in charge of "Privacy Project" in Washington.

Smith also cited the cases of the J.P. Stevens Co., which was accused by the Justice Department of tapping the phones of two former employees it suspected of being union organizers.

The telephone monitoring of employees conversations is quite common throughout the country.

A gray area

In many cases, it's not against the law. It occupies a rather gray area that smacks to the layman of illegality but apparently is not in violation of existing statutes, according to legal experts.

In New Jersey, the Bell Telephone System leases monitoring devices to some 50 customers, most of them commercial firms whose employees have extensive telephone contact with the public. The devices make it possible for supervisors to listen in secretly to conversation between employees and clients.

The Bell system has leased these monitoring devices to some 4,500 subscribers in the United States—mostly large companies and governmental agencies, a Bell spokesman testified earlier this month at a hearing conducted by the House subcommittee on telephone surveillance.

In New Jersey and other

states where the law requires that an employee be warned before he can be monitored, employers often arrange to have their workers sign waivers. In other states, however, companies are not even required to notify workers.

'Hasn't been tested yet'

"The whole issue of telephone monitoring hasn't been tested yet," McCrie said.

Smith, the ACLU lawyer, says that telephone monitoring by commercial firms is part of a trend of general distrust of employees. "We think such practices as wiretapping are going to increase in private industry," he said.

Other electronic devices used to tighten industrial security are not very likely to raise cries of outrage from civil libertarians, however.

Pan Am, for instance, boasts a virtually foolproof system of overlapping TV monitors scanning every inch of cargo loading areas indoor and outdoor, with all the cameras feeding back to a central point.

Track down location

Railroads and some trucking outfits use a magnetically coded strip imprinted along the side of their cabs. The strip is scanned by a monitor at various points and a computer can track down the car's location at any time.

Professionals in industrial security and surveillance are not uniformly convinced of the effectiveness of electronic devices. Gadgets are fine to help guard property, they say, but when it comes to investigation—and espionage or pirating of industrial secrets, for that matter—they prefer to use a much older weapon—people.

"Bugging is a very colorful means of getting information," said McCrie. "But it's neither the most effective nor the most common method used."

Unless a bug is used in conjunction with extremely sophisticated screening equipment to filter out unwanted background noises, the quality of industrial intelligence obtained through it can be so

jumbled as to make it virtually worthless, especially if complex technological processes are discussed.

"When it really comes down to it, technical innovations can make the job of an investigator much easier, but still, a lot of hard work is what investigation is all about. It takes a man with experience and intelligence to put all the pieces together," said Neville, of Pinkerton's.

A spokesman for Burns International Security Services, one of the largest private investigation agencies in the country, with some 36,000 employees, said, "You don't really need bugs when you can find out an awful lot about a company by going through its office trash."

When it comes to pirating sensitive information away from competitors, McCrie said, some companies turn to detective agencies that use seemingly independent employment agencies to place undercover agents in the industry targeted for espionage.

Joe Cataldi, owner of the New Jersey Private Investigation Bureau of Hackensack, the largest of the state's 400 private detective agencies, has nothing but contempt for electronic bugs and their users.

"First of all, the use of a bug is usually the sign of an amateur—and an amateur is a pain in the tail," Cataldi said.

"Bugs are as dangerous as heroin and guns," he said. "The laws governing them are not nearly strict enough. I get requests from clients all the time. The first word out of their mouth is 'We want to tap the ladies' room, or the men's room.' So we tell them we don't do that sort of thing. And they say, 'Who'll know about it?' If the client insists, we dump him."

"When a businessman uses a man to put in a tap, it can turn out to be a double-edged sword. It can come right back and harm him," Cataldi said. "A person deceitful and unscrupulous enough to agree to it won't think twice about exploiting the tap and his knowledge against the same person who hired him."

EXHIBIT NO. 12
THEFT OF TRADE SECRETS

According to a study made by the American Law Division, Library of Congress, theft of trade secrets is prohibited by statute in only three states, New York, California and New Jersey [copies of the statutes attached]. In other states, industrial espionage activities are classified under such headings as theft, burglary, trespass, and wiretapping. While most states have statutes prohibiting unfair competition or unfair trade practices, others include even those offenses under the broad common law categories of trespass or theft.

New York was the first state to pass a statute forbidding the theft of trade secrets, enacting the law in 1964. New Jersey and California passed similar laws within the next three years. All

three of the statutes are broad enough to cover industrial or commercial espionage by breaches of contractual obligations of confidence as well as by theft or wiretapping. The statutes prohibit the theft or unlawful appropriation of 'trade secrets,' generally defined as any information of value to the owner which is not generally available to the public, and do not require use or publication of the secret information.

Confidential business information may be protected under a variety of other theories, including unfair competition, commercial bribery, or acts detrimental to an employer. Remedies under these various theories may include an injunction to restrain disclosure or use of the information, or an accounting of profits derived from unauthorized use.

INDUSTRIAL ESPIONAGE

NEW YORK STATUTE

§ 1296. Grand larceny in second degree

A person is guilty of grand larceny in the second degree who, under circumstances not amounting to grand larceny in the first degree, in any manner specified in this article, steals or unlawfully obtains or appropriates:

1. Property of the value of more than one hundred dollars, but not exceeding five hundred dollars, in any manner whatever; or

2. Property of any value, by taking the same from the person of another; or,

3. A record of a court or officer, or a writing, instrument or record kept filed or deposited according to law, with, or in keeping of any, public office or officer.¹

4. Property of any value consisting of a sample, culture, micro-organism, specimen, record, recording, document, drawing or any other article, material, device or substance which constitutes, represents, evidences, reflects, or records a secret scientific or technical process, invention or formula or any phase or part thereof. A process, invention or formula is "secret" when it is not, and is not intended to be available to anyone other than the owner thereof or selected persons having access thereto for limited purposes with his consent, and when it accords or may accord the owner an advantage over competitors or other persons who do not have knowledge or the benefit thereof. As amended L.1912, c. 164; L.1927, c. 679; L.1964, c. 727, eff. July 1, 1964.

¹ So in original. Probably should read "; or".

§ 1297. Grand larceny in second degree; how punished

Grand larceny in the second degree is punishable by imprisonment for a term not exceeding five years.

NEW JERSEY STATUTE

2A:119-5.1 Crimes involving trade secrets; purpose of act

It is the purpose of this act to clarify and restate existing law with respect to crimes involving trade secrets and to make clear that articles representing trade secrets, including the trade secrets represented thereby, constitute goods, chattels, materials and property and can be the subject of criminal acts.

L.1965, c. 52, § 1, eff. May 17, 1965.

Historical Note

Title of Act:

An Act concerning crimes and supplementing chapter 119 of Title 2A of the New Jersey Statutes. L.1965, c. 52.

Library References

Larceny ⇨2.
Trade Regulation ⇨311.
C.J.S. Larceny §§ 1, 82.

C.J.S. Trade-Marks, Trade-Names,
and Unfair Competition §§ 134,
170.

2A:119-5.2 Definitions

As used in this act:

(a) The word "article" means any object, material, device or substance or copy thereof, including any writing, record, recording, drawing, sample, specimen, prototype, model, photograph, micro-organism, blueprint or map.

(b) The word "representing" means describing, depicting, containing, constituting, reflecting or recording.

(c) The term "trade secret" means the whole or any portion or phase of any scientific or technical information, design, process, procedure, formula or improvement which is secret and of value; and a trade secret shall be presumed to be secret when the owner thereof takes measures to prevent it from becoming available to persons other than those selected by the owner to have access thereto for limited purposes.

(d) The word "copy" means any facsimile, replica, photograph or other reproduction of an article, and any note, drawing or sketch made of or from an article.

L.1965, c. 52, § 2.

Library References

Larceny \Rightarrow 2.	C.J.S. Trade-Marks, Trade-Names,
Trade Regulation \Rightarrow 311.	and Unfair Competition §§ 134,
C.J.S. Larceny §§ 1, 82.	170.
	Words and Phrases (Perm.Ed.)

2A:119-5.3 Theft, embezzlement or copying of article representing trade secret; intent; misdemeanor or

Any person who, with intent to deprive or withhold from the owner thereof the control of a trade secret, or with an intent to appropriate a trade secret to his own use or to the use of another.

(a) steals or embezzles an article representing a trade secret, or,

(b) without authority makes or causes to be made a copy of an article representing a trade secret,

Is guilty of a misdemeanor, if the value of the article stolen, embezzled or copied, including the value of the trade secret represented thereby, is less than \$200.00, and of a high misdemeanor if such value is \$200.00 or more.

L.1965, c. 52, § 3.

Library References

Larceny \Rightarrow 1, 5, 88.	C.J.S. Trade Marks, Trade-Names,
Trade Regulation \Rightarrow 311.	and Unfair Competition §§ 134,
C.J.S. Larceny §§ 1, 1, 158.	170.

2A:119-5.4 Taking of article representing trade secret by force or violence; misdemeanor

Any person who by force or violence or by putting him in fear takes from the person of another any article representing a trade secret is guilty of a high misdemeanor and shall be punished by a fine of not more than \$5,000.00, or by imprisonment for not more than 15 years, or both.

L.1965, c. 52, § 4.

Library References

Larceny \S 1, 5, 8S.	C.J.S. Trade Marks, Trade-Names,
Trade Regulation \S 311.	and Unfair Competition \S 134,
C.J.S. Larceny \S 1-4, 7, 9, 15S.	170.

2A:119-5.5 Certain defenses unavailable

In a prosecution for a violation of this act it shall be no defense that the person so charged returned or intended to return the article so stolen, embezzled or copied.

L.1965, c. 52, § 5.

Library References

Larceny \S 26.	C.J.S. Trade-Marks, Trade-Names,
Trade Regulation \S 315.	and Unfair Competition \S 170.
C.J.S. Larceny \S 71, 72.	

CALIFORNIA STATUTE

§ 499c. Trade secrets; theft; solicitation or bribery to acquire; punishment; defenses

(a) As used in this section:

(1) "Article" means any object, material, device or substance or copy thereof, including any writing, record, recording, drawing, sample, specimen, prototype, model, photograph, microorganism, blueprint or map.

(2) "Representing" means describing, depicting, containing, constituting, reflecting or recording.

(3) "Trade secret" means the whole or any portion or phase of any scientific or technical information, design, process, procedure, formula or improvement which is secret and is not generally available to the public, and which gives one who uses it an advantage over competitors who do not know of or use the trade secret; and a trade

secret shall be presumed to be secret when the owner thereof takes measures to prevent it from becoming available to persons other than those selected by the owner to have access thereto for limited purposes.

(4) "Copy" means any facsimile, replica, photograph or other reproduction of an article, and any note, drawing or sketch made of or from an article.

(5) "Benefit" means gain or advantage, or anything regarded by the beneficiary as gain or advantage, including benefit to any other person or entity in whose welfare he is interested.

(b) Every person is guilty of theft who, with intent to deprive or withhold from the owner thereof the control of a trade secret, or with an intent to appropriate a trade secret to his own use or to the use of another, does any of the following:

(1) Steals, takes, or carries away any article representing a trade secret.

(2) Fraudulently appropriates any article representing a trade secret entrusted to him.

(3) Having unlawfully obtained access to the article, without authority makes or causes to be made a copy of any article representing a trade secret.

(4) Having obtained access to the article through a relationship of trust and confidence, without authority and in breach of the obligations created by such relationship makes or causes to be made, directly from and in the presence of the article, a copy of any article representing a trade secret.

(c) Every person who promises or offers or gives, or conspires to promise or offer to give, to any present or former agent, employee or servant of another a benefit as an inducement, bribe or reward for conveying, delivering or otherwise making available an article representing a trade secret owned by his present or former principal, employer or master, to any person not authorized by such owner to receive or acquire the same and every person who, being a present or former agent, employee, or servant, solicits, accepts, receives or takes a benefit as an inducement, bribe or reward for conveying, delivering or otherwise making available an article representing a trade secret owned by his present or former principal, employer or master, to any person not authorized by such owner to receive or acquire the same, is punishable by imprisonment in the state prison not exceeding 10 years or in a county jail not exceeding one year, or by fine not exceeding five thousand dollars (\$5,000), or by both such fine and such imprisonment.

(d) In a prosecution for a violation of this section it shall be no defense that the person so charged, returned or intended to return the article.

(Added by Stats.1967, c. 132, p. 1164, § 2.)

CALIFORNIA STATUTE (Continued)

Historical Note

Section 1 of Stats.1967, c. 132, p. 1163, provided: "It is the purpose of this act to clarify and restate existing law with respect to crimes involving trade secrets and to make clear that articles representing trade secrets, including the trade secrets represented thereby, constitute goods, chattels, materials and property and can be the subject of criminal acts."

Former section 499c, added by Stats. 1943, c. 793, p. 2580, § 1, and which expired by its own terms September 15, 1945, was repealed by Stats.1963, c. 372, p. 1163, § 11. The former section read as follows:

"Every person who is guilty of the theft of an automobile tire or tires is guilty of a public offense that shall be punished by imprisonment in the State prison for not exceeding five years, or by imprisonment in the county jail for not exceeding one year,

or by a fine not to exceed five hundred dollars (\$500), or both.

"This section shall remain in effect until the ninety-first day after final adjournment of the Fifty-sixth Regular Session of the Legislature or until the cessation of hostilities in all wars in which the United States is now engaged, whichever first occurs. While this section is in effect it shall supersede any existing provisions of law which are in conflict with this section; but such provisions are not repealed by this section and after this section is no longer effective shall have the same force as though this section had not been enacted."

Former section 499c, added by Stats.1909, c. 358, p. 590, § 1, and repealed by Stats. 1933, c. 27, p. 247, § 802, relating to the unlawful use of and to tampering with automobiles, was reenacted as Vehicle Code § 443 (repealed. See, now, Veh.C. § 10851).

Law Review Commentaries

Elghth Amendment rediscovered. Stanley Mosk. (1968) 1 Loyola L.Rev. 4.

Library References

Larceny ⇨2 et seq.

Master and Servant ⇨18, 60, 67.

Trade Regulation ⇨861 et seq.

C.J.S. Larceny §§ 1, 82.

C.J.S. Master and Servant §§ 14, 72, 80.

C.J.S. Trade-Marks, Trade-Names, and Unfair Competition § 237.

Notes of Decisions

1. Legislative intent

The following statement would be consistent with S.B.No.69, which added this section in 1967: "It is intended that the bill not apply to the mobile employee who retains in his mind information and knowledge acquired while in the employ of one employer and uses or gives it in service of a later employer. The intent is to promote the proper development of scientific and technical trade secrets while at the same

time avoiding undue restrictions on the availability of information for which persons in the course of their personal experience have developed or acquired. Thus copies of articles representing trade secrets which are not made at the time that there is access to the article by reason of occupying a position of trust and confidence are not intended to be within the scope of the operation of S.B.No.69." Op.Leg.Counsel, 1967 A.J. 1997; 1967 S.J. 1328.

CHAIRMAN ERICKSON: I think we will adjourn at this time and reconvene at 1:30.

[Whereupon, at 12:30 p.m., a luncheon recess was taken until 1:30 p.m.]

AFTERNOON SESSION

CHAIRMAN ERICKSON: Come to order, please.

[Whereupon, Messrs. Bell, Kaiser, and VanDewerker were sworn by Chairman Erickson.]

TESTIMONY OF PANEL ON COUNTERMEASURE EQUIPMENT: ALLAN D. BELL, JR., PRESIDENT, DEKTOR COUNTERINTELLIGENCE AND SECURITY, INC; MARTIN L. KAISER, PRESIDENT, MARTIN L. KAISER, INC.; JOHN VANDEWERKER, COMMISSION CONTRACTOR; AND BEN JAMIL, COMMUNICATIONS CONTROL CORPORATION, ACCOMPANIED BY PHILIP IEHLE.

CHAIRMAN ERICKSON: Mr. Ben Jamil is not in the room. He is under subpoena, and I believe there is a statement to be made by the investigator regarding Mr. Jamil who was served by the United States Marshal in order to be here.

MR. HERSHMAN: Mr. Chairman, could we perhaps give him the benefit of the doubt and proceed with opening statements and see if he arrives within the next ten minutes?

CHAIRMAN ERICKSON: We will postpone the comments regarding Mr. Jamil for a period of 20 minutes to see if he does arrive, and the record will be dealt with at that point.

It is a pleasure to introduce to you the Panel on Countermeasure Equipment Manufacturers.

Mr. Allan Bell is President of Dektor Counterintelligence and Security, Inc.

Mr. Martin L. Kaiser is the founder of Martin L. Kaiser, Inc.

And with them at the table is John VanDewerker, a Commission contractor, who has worked as a countermeasures specialist with the government.

Mr. Ben Jamil, who hopefully will honor his subpoena, is well-known for his action in this area.

I believe there are opening statements, and if we may look to the time exigencies of the circumstances that face us, I would suggest that if we can we try to limit our opening statements to five minutes.

Mr. Kaiser, would you proceed with your opening statement.

MR. KAISER: Thank you.

Martin L. Kaiser, Inc., was chartered as a Maryland-based corporation in 1965. Its initial objective was to establish a job shop manufacturing facility and provide instrumentation repair for Baltimore industry. Within a year's time, the company had developed an impressive list of clientele which included steel, plastic, material handling and brewing companies.

While attempting to broaden our market area, we accidentally discovered the United States Army Intelligence facility at Ft. Holabird, Maryland. The service we initially provided for this facility was the repair of all forms of intelligence and counterintelligence electronic equipment. Exposure to this equipment resulted in the conclusion that it was generally of poor quality.

Several proposals were made by Martin L. Kaiser, Inc. whereby we would manufacture similar products. Acceptance was almost immediate and our intelligence and counterintelligence product line expanded rapidly. A few of these products were direct field replacement units. However, the bulk were developed by feedback between the agencies and myself. This general manufacturing area represented such an interesting challenge that we subsequently withdrew our efforts in the repair of commercial equipment. Through word-of-mouth advertising, our customer list grew until it included nearly every federal intelligence agency. By mere association, our products spread downward through state and local governments.

In mid-1968 I was made aware of the existence of the new Public Law 90-351. The law seemed clear and concise, and did not deviate much from what I had already established as company policy. The law clearly stated that it was illegal to advertise, assemble, manufacture, possess or sell an electronic surveillance device. From a purely manufacturing standpoint, the law was a blessing primarily because it built in the element of time. Also, since it restricted possession, it meant that we now had only to purchase those components necessary to produce the devices presently on order.

The law also meant, from a marketing standpoint, that it was no longer necessary to gauge market trends or build inventories. Increased costs due to limited production runs could now be readily passed on to the consumer.

One of the side benefits of the law, and one which I personally feel was of great value was that it frustrated, by inserting the element of time, the heat of passion. It now meant that agencies and agents had to carefully evaluate their plans concerning the use of electronic surveillance equipment.

For years, the issue of manufacturing prior to receipt of proper authorization was frequently brought to my attention. In most cases, the warnings were moot because, in agreement with the law, we restricted distribution of our literature; we never had advertised our products and we had, in the past, only manufactured to order.

In 1970, we became aware of the formation of a Florida-based surveillance product manufacturing firm. This company promptly printed an expensive and impressive catalog devoted solely to electronic surveillance equipment, built a huge inventory and boasted of same and began a national advertising campaign. In short, they did everything which I had been specifically instructed not to do.

I brought their actions to the attention of the Justice Department only to be advised not to attempt to use them as my private attorneys. Attempts to involve both of the good Senators from the State of Maryland and my Congressman in this matter resulted in the same basic response coupled with a Justice request for more funds to keep their department operating smoothly. As you can clearly see from the records supplied you, the impact of this Florida-based company on my surveillance product line has been disastrous.

We are now here before you to consider, among other things, the possibility of licensing or other-

wise controlling the manufacturers and users of electronic countermeasure equipment. Needless to say, I am very concerned because I clearly foresee a repetition of the unfair action given me under the Omnibus Crime Bill.

Martin L. Kaiser, Inc., was one of the very first companies to make a concerted effort in the design and manufacture of the general-purpose countermeasure equipment, and I trust that you will agree with me that the need for creative development in this area is still essential. It is, indeed, a pity to observe the influx of 'snake-oil salesman' and charlatans into the electronic countermeasure business; however, as it has been said for centuries, caveat emptor.

The object, therefore, in my opinion, is to allow the marketplace to control itself. Advertising which contains little truth seems to be the avenue most used by those who wish to market a product of questionable attributes. Perhaps reenforcement of already existing regulations relating to truth in advertising might prove useful.

I am looking forward to an open and frank discussion of these issues.

Thank you.

[Material relevant to the above discussion follows.]

MARTIN L. KAISER, INC.

ELECTRONIC COUNTERMEASURE EQUIPMENT



1040 COUNTERMEASURE KIT

The 1040 contains all the necessary "tools" for a complete RF and Audio survey. Kit includes: two 1059 general purpose amplifiers with headsets, 2030 carrier current probe, 2050 CA RF locator with visual and tonal readouts, 2040 test oscillator, 1040-1 general purpose microphone, 1040-2 contact microphone, 1040-3 tone probe, 1040-4 hot pack, multimeter, patch cables, tool set, fuse puller, two lanterns with adjustable focus, cable adapter set, radio (known noise source) and instruction manual. All above housed in standard 5x12x18" attache with foam insert. Insert has sufficient cutouts for 8010 or 8010C metal locators.

- - - -



1080D TELEPHONE ANALYZER

The 1080D is a completely self-contained battery operated unit designed to counter alterations to telephone and intercom systems. Features: High gain audio amplifier with switchable amplification ratio and input impedance. RF detector for broadband detection from 20 kHz to over 500 MHz and tuneable detection from 500 kHz to 200 MHz. Unit has tonal/visual readout to pinpoint RF sources. Tone generator for detection of tone activated devices. Capacitance detection and relative measurement circuit. High voltage generator supplies 0-1000 VDC for detection of special devices. Pulse generator for capacitor detection and locating special attacks.

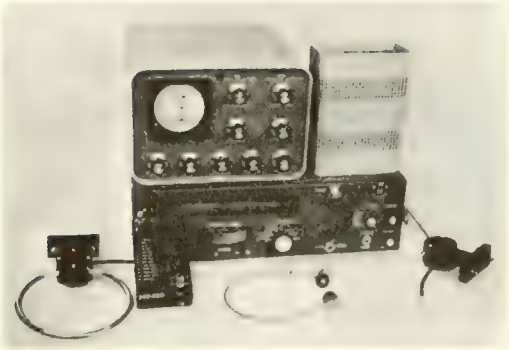
Three meters for measuring DC voltage, current, relative RF and capacity. Uses two standard 9 volt batteries and two 500 volt batteries. Supplied in standard 5x12x18" attache. ACCESSORIES: TA1080LE line extender. Mates 50 pin plug on standard key telephone to analyzer. Provides every possible pair combination.

TA1080RAC rechargeable power pack. Installs within analyzer and supplies both high and low voltages. Designed for use where large quantity testing is done.

MARTIN L. KAISER, INC.

ELECTRONIC COUNTERMEASURE EQUIPMENT

6060 RECEIVER SYSTEM



The 6060 countermeasure receiver system is supplied with a general coverage receiver, high frequency converter, sub-carrier detector, panadapter, antennas, headset, patch cables and carrying cases. Receiver and accessories are in one case and panadapter and accessories in the other. Cases are standard "Carry On" one suiters.

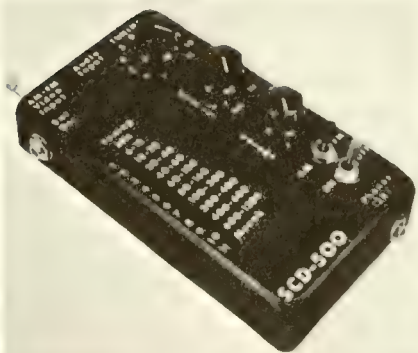
The system covers 6kHz to 1800mHz and has subcarrier detection from 550kHz to 1800mHz. Subcarrier detection from 50kHz to 1800mHz is available with optional extender 6070. Input of 1uV gives $\frac{1}{2}$ "

amplitude display on panadapter. Receiver features field strength meter for accurate signal location and loudspeaker for feedback detection techniques. Panadapter has fixed bandwidths of 10 and 50kHz and variable bandwidth of 60 to 600kHz. Resolution is approximately 500Hz. Variable vertical amplitude is either linear (10:1), log (100:1) or log -20 DB (1000:1). Power is batteries for receiver, converter and subcarrier detector and 110 or 220 VAC 50/60Hz, 45 watts. Please specify voltage. AC and 12 VDC model also available.

- - - -

SCD 500 SUBCARRIER DETECTOR

Designed for detection of subcarriers located 6 to 1200kHz from main carrier. May also be used as direct conversion low frequency receiver with ACA/SCD adapter. Uses video output of R200P, 3075, 3075A or 6060 receiver. Inputs: AM-FM Video (or direct RF), receiver audio and external BFO (if desired). Output: 2000 ohms to headset. Controls: Tuning, Vernier Tuning, Volume, AM-FM Demodulator, and Power ON/OFF. Powered by two 9 volt batteries. Case size 3/4x3x5". Requires VAC/SCD cables for receiver interconnect.



PROPRIETARY INFORMATION
STANDARD TERMS AND CONDITIONS APPLY

CHAIRMAN ERICKSON: Mr. Kaiser, thank you.

Mr. Bell.

MR. BELL: Mr. Erickson, my prepared opening statement goes considerably beyond five minutes. I understand this has been provided to the Commission.

CHAIRMAN ERICKSON: Yes. I ordered on behalf of the Commission yesterday that all opening statements and documents are made a part of the record in this proceeding. So if you could summarize it, Mr. Bell, we'd be very grateful.

MR. BELL: Yes. I will leave out some of the justification for the recommendations I make but touch on them briefly.

I have addressed the law from the standpoint of what I perceive to be the intent, that is, what it accomplishes for the citizens. I think the law was well-researched and well-written, but I don't believe it has fulfilled the intent. And I think there are a couple of basic problems with this that could be addressed and could be overcome.

First of all, the law prohibits two things. One is specific equipment designed primarily for the interception of oral communications, and secondly the act, regardless of the equipment.

The prohibition of the equipment under the law has not resulted in the nonavailability of equipment that will do the eavesdropping job for the average citizen or even for more sophisticated personnel.

For every type of eavesdropping there is a legal, readily available piece of equipment that will fulfill the function. I have some examples here with me if the committee would care to see these.

The problem with controlling the action is the problem that exists with every law, and that is the enforcement.

This type of a crime is the type of crime that almost absolutely has to be detected in the process of its commission. As our expert on computer tapping pointed out today, there is no evidence which remains after the crime has been committed. In almost every other crime, there is a corpus delicti which results. Even embezzlement, which is a secret sort of stealing, ultimately leaves the funds which are missing as an indication that the crime has been committed.

From the citizen's standpoint, there are no mechanisms within the federal agencies, or in most cases within state agencies, to allow them to get countermeasure surveys of their offices or their homes in an effort to detect the crimes under commission.

So in spite of the law and the very reasonable prohibitions it provides, ultimately, as far as the average citizen is concerned, or businessman, he

has nothing in the law or in support of the law that is going to fulfill the function of keeping him from having his information acquired.

Traditionally, before the law and since, this function has been fulfilled by private organizations, individuals, entrepreneurs, that provide this service for a fee. And I would like to divide these up into three categories: sincere and effective; sincere and ineffective; and charlatans.

Now, there are, of course, shades of gray in these, degrees of sincerity and degrees of effectiveness.

I feel that there is legislation which is required. I feel there are controls which need to be exercised to influence the quality of what is provided the citizen in this very sensitive requirement he has for which he is paying his money.

And I would like to run over that list of recommendations:

1. Establish functional countermeasures equipment standards for each of three levels of capability—high, medium, and low. Establish or designate a facility for testing equipment currently manufactured and new equipment as it may be developed to determine the specific threats such equipment will detect or prevent and its level of effectiveness.

2. Establish procedures whereby this testing facility may receive data concerning new threats in order that standards may be revised as required.

3. Periodically publish equipment evaluation reports so that countermeasures services personnel, current and future, and the public may be informed of the validity of the equipment they will use or have used for them.

4. Require that countermeasures services personnel inform potential clients, in writing, of the determined capabilities and limitation of the equipment and procedures to be used for the services they are offering.

5. Require that countermeasures services personnel and companies offering such services clearly state in any advertising the determined capabilities and limitations of the equipment and procedures they will use in performance of the services.

6. Require that countermeasures equipment manufacturers and sales personnel provide to prospective buyers a written statement of the determined capabilities and limitations of the equipment they are offering for sale.

7. Require that any advertising accomplished for the sale of countermeasures equipment include a clear statement of the determined capabilities and limitations of the equipment being offered for sale.

8. License eavesdropping countermeasures service personnel based upon written examination in the manner of Federal Communication Commission examinations for radio operators.

The second part of the problem with the law is the comprehensiveness of the prohibition of possession. And I believe there are several areas in which it is not only reasonably permissible to possess under control, but is advisable.

One of these has to do with research and development of countermeasures equipment. It is with some difficulty that one researches a countermeasure to something when he is not able to lay his hands on the devices he is building a countermeasure against.

My second is one which the gentleman from Hewlett-Packard pointed out the need for, and that is a means of training individuals to comply with standards and requirements within their capabilities.

At the present time, in order to train, systematically train, one does not have or is not allowed to have the equipment which could be used for a dynamic training process. I believe this also should be allowed under controls, and there are several others which are reflected in my last recommendations here.

But each of these, I think, would involve licensing, establishing of controls, and accountability for specific devices for specific purposes which fulfill ultimately, or tend to fulfill, the intent of the law, and that is, bring the standards up, get the people trained, enhance the research and development effort in the countermeasures equipment, and in general attack the entire problem.

Thank you.

CHAIRMAN ERICKSON: Mr. Bell, I appreciate that very much.

[Mr. Bell's prepared statement follows.]

STATEMENT OF ALLAN D. BELL, JR.

PRESIDENT, DEKTOR COUNTERINTELLIGENCE AND SECURITY, INC.

I am Allan D. Bell, Jr., President and Chairman of the Board of Dektor Counterintelligence and Security, Inc., a privately-held corporation structured to perform informational research and material research and development in problem areas of counterintelligence and security. Our products are procedures, techniques, training, services, and equipment. The bulk of our activities are directed toward eavesdropping countermeasures.

In this opening statement I will address problems that have developed with the law under study by this Commission.

First of all, let me state that I consider the law to have been well researched and written. It comprehensively covers the intended area, that is, it provides the basis for control of illegal eavesdropping, as defined by the law. It is sufficiently moderate in its approach, in recognizing the right of an individual to record what he can hear, just as he is allowed to photograph what he can see. The requirement for court order for technical eavesdropping by law enforcement agencies appears completely consistent with current interpretations of Fifth Amendment rights and rules of evidence.

The problems I perceive are in two areas: (1) Execution and enforcement of the law and (2) restrictions on possession of equipment under circumstances not involving eavesdropping, where some modification of the restrictions may ease problems beyond the apparent intent of the law and, in some cases, further the intent of the law.

I will address these two areas separately and will provide my recommendations to deal with each of them.

First the problems of enforcement. There are two categories of crimes treated in the law. One has to do with *devices* primarily intended for illegal interception and the other with the *act* of interception. The first promised, at least, to deny to the average citizen devices which could allow him to spy on his neighbor by making it manifestly illegal to have anything to do with such devices, provided they were primarily intended for the illegal interception of voice communication, and thereby remove his means of accomplishing the act of eavesdropping. This promise has not been fulfilled. While it is now indeed difficult for the average citizen to purchase equipment primarily intended for illegal interception, the ability of the average citizen to listen to his neighbor is hardly deterred. Legal equipment, openly advertised and sold, completely satisfies his purpose. Such equipment includes tiny 'entertainment-type' radio transmitters, small transceivers, wireless intercoms, equipment for automatically recording telephone conversations, and battery-operated tape recorders. Drawing the line between devices primarily intended for illegal interception and those not so intended depends, in part, on interpretations of intention. It is difficult. Justice Department has found it to be difficult. There are, of course, some devices that fall clearly into the illegal category; for example, series parasitic radio transmitter telephone taps. There would seem to be no legal purpose for these devices and they have disappeared from the open consumer market. On the other hand, the same results can be attained with legal consumer equipment. While it should be illegal for unauthorized persons to purchase or to possess illegal devices, this element of the law alone will not significantly decrease the acts of illegal eavesdropping.

This leads us to the second category—the crime of the act of technical eavesdropping, regardless of the legality of the devices or equipment employed. This act, as is the case with many espionage techniques, is a secret crime to the fullest extent. Other crimes may be planned secretly, and executed secretly, but eventually there will be a discovery of the crime. Murder, assault, burglary, even embezzlement, leave glaring indications or absences, over and above discovery of tools or devices employed, that tell the discoverer clearly that a crime has been committed. The acquisition of sound leaves no such indication or absence. The crime of eavesdropping usually must be discovered in process. It is almost never discovered after the act has been completed.

While some agencies of the executive branch maintain capabilities for the technical detection of illegal interception, none offer this service to the public. Some police departments have similar capabilities for their own in-house purposes, but again, they do not normally offer this service to the public.

Since the illegal equipment provisions of the law do not prohibit usable equipment, and since the nature of the crime of illegal eavesdropping usually requires that it be detected during the act, and since the official agencies do not and probably cannot offer detection services, the laws offer little to the security of the conversations of the public sector. Rather, individuals and organizations turn to private practitioners of eavesdropping countermeasures to detect or prevent compromise of their private verbal communications. While this approach to security is feasible, the lack of controls which exists today leaves its validity questionable, as well.

The public today has little or nothing available to allow it to evaluate either the nature of the eavesdropping threat or the proposed solutions. Most public knowledge derives from ficti-

tious portrayals in motion pictures, television, and spy novels. Some come from the news media, which tends, in this case, to highlight the improbable. Thus, the public may be misinformed or, certainly, only partially informed concerning the eavesdropping threat. The public has even less basis for evaluating eavesdropping countermeasures.

To resolve its eavesdropping problems, the public turns to so-called specialists in this field, much as a sick person turns to a medical specialist. While the medical specialist must have achieved levels of education and experience, there is currently no means by which the average citizen can determine competence in the area of eavesdropping countermeasures.

With some types of service, it is possible to evaluate the results of the service provided. If one's car will not start, one has it repaired and one can determine if the mechanic who repaired it was successful in correcting the situation. When the eavesdropping countermeasures technician performs his survey and announces that there are no listening devices, the client has no means of determining whether there are, in fact, no devices planted, or whether the technician is incompetent and was unable to find them. Unfortunately, the client who has been given assurance that he is not bugged may cease applying his previous caution with his conversations and will be the worse for having the service performed.

Those persons plying the trade of eavesdropping countermeasures services today may be categorized generally into three groups, with some overlap between the groups and some shades of grey within the groups: (1) sincere and competent; (2) sincere and incompetent; and (3) charlatans. The same three groupings may be applied to manufacturers of eavesdropping countermeasures equipment.

Sincerity is a personal characteristic which is difficult to legislate; however, insincerity more often develops as a cover for incompetence. If competence is required, sincerity is more likely to follow.

Competence on the part of persons who provide countermeasures services, is based on having the required knowledge and the appropriate equipment. Some considerable opportunity for trade-offs exist between required levels of individual knowledge and the validity and comprehensiveness of the equipment they will employ. A mechanic with an ignition analyzer can tune a car better than a graduate mechanical engineer without one, and, in fact, as well as a graduate mechanical engineer with one. The mechanic must have a basic knowledge of automotive ignition and must know how to employ the analyzer. The analyzer must be designed to fulfill its function with validity and reliability. Its limitations, if any, must be understood. In many respects, the same principles apply in eavesdropping countermeasures, particularly when standards are to be established. It is far more feasible to determine the fulfillment of standards with mass-produced equipment than with individual human beings, provided the fulfilled equipment standards satisfy the functional countermeasures requirements.

In any event, both individual and equipment standards are needed, along with a means of enforcing them. The American Society of Testing and Materials, in its Committee F12-70.7 has devoted some considerable study to this problem, particularly the equipment aspects of it. The Committee has addressed the fact that there are different levels of threat and that there should be identifiable levels of eavesdropping countermeasures competence. To provide the highest level of countermeasures to the lowest level of threat becomes excessively expensive. To apply the lowest level of countermeasures against the highest level of threat is futile.

While I recognize the need for both individual and equipment standards for eavesdropping countermeasures and will recommend necessary licensing and controls, I recognize also the problems inherent in establishing valid standards. In order to serve the public need, the standards must be sufficiently specific

and comprehensive to assure that the various threat techniques are addressed. The standards must be stated in *functional* terms to allow and promote the realization of new and better approaches. They must provide for rapid modification in order that they remain valid in a world of dynamic technological advances in the threat. And, finally, the standards must be based upon threat, existing or foreseen, not upon the problems that the standards will cause a manufacturer whose equipment does not qualify.

If controls can be established over countermeasures services and countermeasures equipment, the effectiveness of what I perceive to be the intent of the law, i.e., protection of the private conversations of the public, can be vastly enhanced. I submit the following recommendations to this end:

1. Establish functional countermeasures equipment standards for each of three levels of capability (high, medium and low). Establish or designate a facility for testing equipment currently manufactured and new equipment as it may be developed to determine the specific threats each equipment will detect or prevent and its level of effectiveness.

2. Establish procedures whereby this testing facility may receive data concerning new threats in order that standards may be revised as required.

3. Periodically publish equipment evaluation reports so that countermeasures services personnel, current and future, and the public may be informed of the validity of the equipment they will use or have used for them.

4. Require that countermeasures services personnel inform potential clients, in writing of the determined capabilities and limitations of the equipment and procedures to be used for the services they are offering.

5. Require that countermeasures services personnel and companies offering such services clearly state in any advertising the determined capabilities and limitations of the equipment and procedures they will use in performance of the services.

6. Require that countermeasures equipment manufacturers and sales personnel provide to prospective buyers a written statement of the determined capabilities and limitations of the equipment they are offering for sale.

7. Require that any advertising accomplished for the sale of countermeasures equipment include a clear statement of the determined capabilities and limitations of the equipment being offered for sale.

8. License eavesdropping countermeasures service personnel based upon written examination in the manner of Federal Communications Commission examinations for radio operators.

The second area of consideration involves restrictions under the law which, in some circumstances, do not appear to be required to fulfill the intent of the law and may even negate intended results. These are the complete comprehensiveness of restrictions on manufacture, advertising, sale and transportation of eavesdropping devices.

As the law currently exists, it appears illegal for persons or companies involved in research and development of eavesdropping countermeasures techniques and equipment to purchase or possess devices to be used as threat models for development and testing. This frequently requires that countermeasures equipment be developed against hypothesis and leads to inadvertent oversights. It is one of the reasons some of the countermeasures equipment sold today is not effective or as effective as it should be.

As the law currently exists, it appears illegal to conduct an eavesdropping countermeasures training course on a practical application level. For effective countermeasures training, eavesdropping devices are necessary in the demonstration, practical application, and examination phases of the instruction. We see the need for improving the effectiveness of countermeasures ser-

vices, yet the law greatly limits our ability to improve the effectiveness of the personnel who will accomplish such services.

Next, the law provides for sale of eavesdropping devices to exempted agencies and apparently approves the legal use of such equipment. Yet, if a manufacturer obeys the letter of the law, it is difficult, if not impossible, for the exempted agency to see what it may be buying or to witness a demonstration. The problem is perhaps greater when a new, better device could be developed. For the manufacturer to be legal, the customer is required to buy a pig in a poke. While larger federal agencies may be able to fund purchases for test and evaluation, small police departments cannot.

Along the same lines of sales to exempted agencies is the prohibition of manufacturing except in direct fulfillment of a specific purchase order from an exempted agency. Except for the larger federal agencies, most orders could be expected to be for one or two of an item. Setting up for a production run and testing of one or two items is expensive and the expense must be passed on to the exempted agency making the purchase.

Lastly, there is a problem which affects the manufacturer solely. This has to do with overseas sales. The law does not appear to address anything other than domestic sales. Overseas sales were already controlled by State Department, Munitions Board, and Bureau of Commerce, all of which operated in an approval or disapproval capacity. The restriction of sales to an exempted agency, in this case, appears to mean that an exempted agency must become *ade facto* wholesaler in order for an overseas sale to be legally consummated by a U.S. manufacturer.

I am in complete agreement with the intent of the law to control and restrict eavesdropping devices to prevent their illegal use, but to control in a manner which degrades the effectiveness of eavesdropping countermeasures equipment and service personnel appears counterproductive; to control in a manner which

greatly increases the cost to the legal purchaser seems wasteful; and to control in a manner which essentially prohibits export sales seems beyond the scope of this law.

The following recommendations are made to provide for alternative control provisions to deal with these problems:

1. License individuals or companies involved in eavesdropping countermeasures research and development, and provide for their purchase, registration, possession, and accountability of eavesdropping devices for countermeasures research and development purposes.

2. License countermeasures training schools and provide for their purchase, registration, possession, and accountability of eavesdropping devices as training aids.

3. License manufacturers of eavesdropping devices and:

- a. Establish provisions whereby licensed manufacturers and their sales personnel may possess registered devices for purposes of demonstration to the exempted agencies. Require accountability.

- b. Establish provisions whereby licensed manufacturers may make production runs and maintain shelf stock of eavesdropping devices in order that the economics of normal manufacturing processes may be practiced legally with these products. Require accountability.

- c. Establish provisions whereby licensed manufacturers may manufacture and ship eavesdropping devices to foreign destinations subject to normal State Department, Munition Board, and Bureau of Commerce controls, without requiring an exempted agency to agree to become *ade facto* wholesaler. Require accountability.

This completes my opening statement. I will be happy to entertain discussion or questions on these points or any others which may be of interest.

The Threat

Perhaps the most insidious and least recognized method of eavesdropping on room conversations is the modifying of a telephone to convert it to a continuous listening device, even when it is hung-up. These techniques are known as telephone bugging, as opposed to telephone tapping, which involves merely the listening to on-going telephone conversations. Eavesdropping on telephone conversations is indeed a threat; however, far more critical information is frequently uttered after the telephone call has ended. While some care can be exercised over what is said during a telephone conversation, similar precautions against telephone bugging would cripple office efficiency.

There are a variety of different techniques which may be used to bug a telephone, ranging from very simple to very sophisticated. Generally, the threat level equates to the value of the information; in any given situation, however, the full range must be considered as a possibility.

Telephone Analysis

The technique for detecting eavesdropping modifications of the telephone instrument is known as telephone analysis. The telephone is disconnected from the telephone line and subjected to specific tests to determine if modifications have been made. Telephone analysis is sometimes referred to as "off-line testing," as compared to "on-line testing," in which the telephone line is checked to detect an in-use telephone bug or the presence of a telephone tap.

There are three elements involved in telephone analysis: sequencing, detection, and resolution. Most simply stated, sequencing is the process of arranging the conductors exiting from the telephone in all their permutations so all possibilities may be tested; detection is determining that an interconnection exists between conductors; and resolution is determining the nature of that interconnection.

Dektor Telephone Analyzers inherently provide progressive sequencing for the two, three, or four conductors exiting from a single-line telephone. Multiline telephones with up to 255 conductor possibilities are handled by an ancillary sequencing logic unit, which will be discussed subsequently.

There are two general approaches to the detection element. Historically, detection equipment has been designed against specific telephone bugs. This approach has the disadvantage of presupposing that all bugging tech-

niques are known to the design engineers and that no new techniques will be developed. The Dektor approach detects minor deviations from the telephone norm, which will occur when any usable modification to the telephone is made, whatever technique is or may be employed, now or in the future. The effectiveness of the Dektor approach allows us to make the following two challenges:

1. There are some telephone bugging techniques in actual use today that are detectable only by Dektor analyzers.
2. Dektor's DTA and TA-300 analyzers will detect any telephone bugging modification that will produce audio. Dektor's TA-200 will accomplish the same, with the exception of one very specialized technique.

Resolution of the detected connection between conductors is necessary because there may be normal interconnections in the telephone. The minimum resolution acceptable is the determining whether the detection is a normal interconnection. Optimum resolution will determine qualitatively and quantitatively the nature of the interconnection, normal or applied. Dektor's Digital Telephone Analyzer allows the accomplishment of the latter; the TA-300 and TA-200 allow accomplishment of the former.

One additional aspect of telephone analyzer evaluation is simplicity of operation and the degree of training, knowledge, and experience required for the use of the equipment. At Dektor, we engineer the knowledge and experience into our equipment. This avoids extensive training requirements and inadvertent oversights on the part of the user.

DIGITAL TELEPHONE ANALYZER (DTA)



dektor

COUNTERINTELLIGENCE AND SECURITY, INC.

703 569-2900

5508 Port Royal Rd., Springfield, Va. 22151

MODULAR TELEPHONE COUNTERMEASURES

The Dektor Telephone Analyzers TA-300 and TA-200 are the basic components of economical but comprehensive modular systems for telephone analysis, far surpassing standard equipment for the detection of techniques for modifying a telephone to eavesdrop on room conversations.

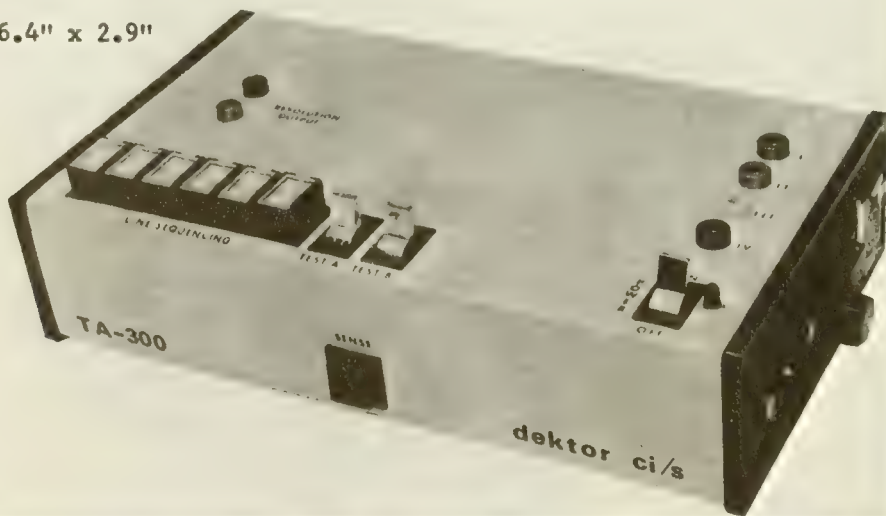
TELEPHONE ANALYZER, TA-300, containing the full Dektor detection circuitry (Test A and Test B), provides simplified hit resolution by means of any external jacked-in multimeter, digital or d'Arsonal, to determine whether the hit is a normal telephone interconnection or an unauthorized modification.

The remaining test and resolution functions are fulfilled by the Polytonic Sweep/Amplifier PSA 250. Full expansion of the system for multi-line telephone capability is achieved with the final component, the Sequencing-Logic Unit (either model SU-400 or SU-300).

See accompanying chart for comparison of TA-300 System with DTA and TA-200.

POWER: Switch Selected,
120/220V AC, 50/60 Hz

SIZE: 10.4" x 6.4" x 2.9"



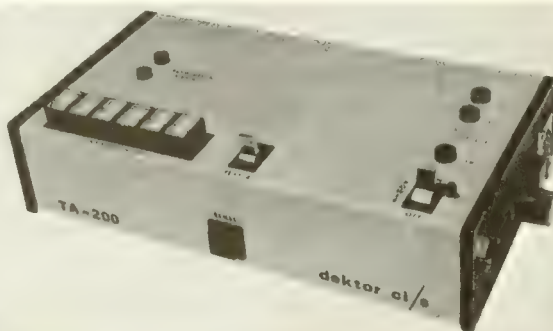
TELEPHONE ANALYZER, TA-200, identical to the TA-300 in all other respects, omits the Test B function which detects the ultra-sophisticated stacked high-voltage four-layer solid-state switches exceeding 1000V breakdown voltage. Test A will detect such devices up to 1000V and all other techniques for telephone bugging.

The TA-200 allows an additional savings in equipment cost by acceptance of a calculated risk for the highest sophistication of attack.

As with the TA-300, resolution is accomplished by any externally connected multimeter and full on-line testing functions are fulfilled with the meter and the addition of the Polytonic Sweep/Amplifier PSA-250. Expansion of the system for a multi-line telephone capability is economically achieved with the Sequencing-Logic Unit SU-300. The entire TA-200 System (TA-200, SU-300, PSA-250, and multi-meter) will fit in one standard 5" attache case.

See accompanying chart for comparison of TA-200 with TA-300 and DTA.

SIZE: 10.4" x 6.4" x 2.9"
POWER: Switch Selected
120/220 V AC, 50/60 Hz



COMPARISON OF DEKTOR TELEPHONE ANALYZERS

	<u>DTA</u>	<u>TA-300</u>	<u>TA-200</u>
OFF-LINE			
<u>Detection Tests</u>			
Resistances	YES	YES	YES
Capacitances	YES	YES	YES
Inductances	YES	YES	YES
Voltage Breakdown			
devices: to 1000V	YES	YES	YES
to 6000V	YES	YES	NO
<u>Resolution Tests</u>			
Vector-scope	YES	NO	NO
Resistance	DIGITAL	EXT MM *	EXT MM *
Capacitance	DIGITAL	NO	NO
Microphonics	YES	NO **	NO **
ON - LINE			
Voltage	DIGITAL	EXT MM *	EXT MM *
Current	DIGITAL	EXT MM *	EXT MM *
Amplifier	YES	NO **	NO **
Polytonic Sweep:			
single-tone bug	YES	NO **	NO **
multi-tone bug	YES	NO **	NO **

* Read-out from any external jacked-in multimeter

** Attainable with Dektor Polytonic Sweep/Amp, PSA-250

dektor

703 569-2900

COUNTERINTELLIGENCE AND SECURITY, INC.

5508 Port Royal Rd., Springfield, Va. 22151

CHAIRMAN ERICKSON: I believe Mr. Jamil was delayed a few minutes and has now arrived.

Mr. Jamil, would you please come forward? Would you be sworn, please.

[Whereupon, Mr. Ben Jamil was sworn by Chairman Erickson.]

CHAIRMAN ERICKSON: Do you have an opening statement?

MR. JAMIL: Yes, it is being distributed now.

CHAIRMAN ERICKSON: The floor is yours, sir, if you'd like to proceed with your opening statement.

MR. JAMIL: My name is Ben Jamil and I am with Communication Control Corporation.

Please forgive me for being late. The taxicab was late bringing me from the airport.

CHAIRMAN ERICKSON: We can understand the difficulty.

May I ask who is with you?

MR. JAMIL: This is Mr. Phil Iehle, consultant to our company.

CHAIRMAN ERICKSON: Will he be testifying as well?

MR. JAMIL: Yes.

[Whereupon, Mr. Philip Iehle was sworn by Chairman Erickson.]

CHAIRMAN ERICKSON: You may proceed, Mr. Jamil.

MR. JAMIL: Wiretapping and eavesdropping are more prevalent now than ever before. One need only go to the friendly neighborhood electronics store and pick up any items that fall into categories as transmitters, wireless intercoms which can be used for bugging, simple monitoring devices, parabolic microphones, wireless microphones supposedly used for musical purposes but are really used for monitoring.

And if these items aren't satisfactory, you can go to a number of stores and buy a telephone—complete with a tap.

Does this sound frightening? It is. Because it marks the breakdown of enforcement of the laws preventing the manufacture and distribution of illegal bugging and eavesdropping devices.

In our opinion, legislation is next to meaningless.

The passage of new laws, no matter how well-meaning, can't really stop illegal surveillance. Only well-organized and thorough law enforcement can do that. The situation today is this: Anybody can buy an inexpensive device in any one of perhaps thousands of radio, electronic, TV supply stores. These can be planted in an office or home and safely monitored while parked blocks away.

This same untrained nontechnician could spend \$200 for a device known as the infinity transmitter which takes a few minutes longer to install. Then

this fellow could call your telephone number from anywhere in the continental United States and listen to conversations taking place in your board room, your office, even your living room, without being detected. As you know, the telephone does not ring, nor does the telephone call register on the telephone bill.

Let me assure you people that the new, good bugging devices we are encountering are becoming more and more sophisticated. We have seen factories in England and the Continent that are working busily with extra shifts to manufacture extraordinarily sophisticated devices which are then shipped into the United States in cartons bearing innocent labels like: 'Babysitter,' 'Alarm Systems,' 'Intercoms.'

You probably have seen examples of clandestine listening devices. Our distributors have found numerous numbers of drop-in transmitters that broadcast two sides of a telephone conversation, and they resemble, identically in some cases, the standard telephone mouthpiece capsules.

Fountain pen transmitters—we saw in operation being manufactured in London innocent looking fountain pens which, when placed on an executive's desk, would pick up all conversations within 15 feet and broadcast 600 feet away to an eavesdropper listening in a car.

We saw wireless microphone transmitters that broadcast a few hundred feet that require no batteries, no power whatsoever. They draw their power from the energy of a near-by radio or television broadcasting station. And these transmitters operate for an indefinite period of time.

We came across a new breed of infinity-type transmitters which, as we said, allow the eavesdropper to monitor the room conversations—undetectable. There is no way whatsoever of detecting any of these infinity-type transmitters because they are triggered with the use of two, four, and six different type tones, rendering them completely undetectable to any piece of equipment in the countermeasure field.

These are some of the few extremely sophisticated and intricate devices, and I think the trend is toward even greater sophistication. I am sure you all have read of some of the Soviet intelligence in monitoring U.S. electronic intelligence that enters the extensive microwave relay network between satellites and between radio relay stations.

The *Chicago Tribune* recently quoted a source as estimating that the number of calls monitored by Soviet intelligence ranged into the hundreds of thousands, even millions, of telephone conversations.

The American Telephone and Telegraph Company monitored millions of long-distance calls in the United States between 1965 and 1970 as part of the campaign to stop cheating on toll charges. It has been estimated that AT&T monitored more than 30 million calls in random fashion. Obviously, between the Soviets, AT&T, and the plain ordinary criminal eavesdropper, it has become increasingly difficult to have the luxury of a private telephone conversation.

The 1968 Omnibus Crime Control and Safe Streets Act made it illegal to manufacture, sell, purchase, possess or use electronic eavesdropping equipment except by law enforcement bodies, and then only by court order.

But the law was almost immediately watered down by judicial rulings allowing employers to tap the telephones of their employees if the phone calls went through a company's switchboard. I have heard that more rulings have effectively destroyed the law's intent.

But, no matter. For how does one outlaw a microphone, a transmitter, an FM radio or receiver? How does one outlaw a tape recorder?

Most important of all, the passage of this law was perhaps the single most influential factor in publicizing, promoting, and instigating the usage of bugging equipment this nation has ever known.

When the *Washington Post* began its investigations into the Watergate affair, Democrats were not able to influence the American voter that anything illegal or even immoral had taken place. After all, what was so abnormal about the leakage of information in political warfare? Is not every adult subject to mysterious methods of investigation and scrutiny when buying insurance, when applying for credit, and when looking for a job?

It was only at the climax of the Watergate affair that the moral implications became clear to the general population.

The trade magazine, *Industrial Security*, states that the average American tends to think eavesdropping is something that happens to the other fellow, that it could not possibly happen to him. It is this naive attitude, they report, that makes electronic eavesdropping an easy task for the business or industrial spy, for the act of bugging or tapping is far from mysterious magic.

They offer facts that one can be overheard in the privacy of one's home, office, phone booth, a street corner, driving in one's car, and even in a boat in the middle of a lake. They state that many people tend to disregard the threat, not only because it couldn't happen to them but also because they feel incapable of doing anything to combat eavesdropping. Bugging equipment is on the open mar-

ket. It is cheap, effective, and there are no serial numbers or other markings to trace.

My company is in business to combat the 'bug.' We do it in three ways:

We design, develop, manufacture and distribute a whole line of equipment for the use of private, industrial, and government security personnel. This equipment includes secure telephones, automatic transmitter bug detectors, telephone analyzers and full antisurveillance kits. We feel this is sophisticated equipment designed to combat the electronically sophisticated 'bugger'. And when I complete my statement I will demonstrate this equipment and answer questions concerning it.

A very important part of our program is education. We conduct seminars for security professionals in order to acquaint them with the state of the art in illicit surveillance techniques and antisurveillance techniques.

We think that education is the real answer as opposed to a better mouse trap, a better debugger, a more sensitive receiver or more fancy machine.

Most people live in a quandary, in a state of confusion. They don't even know what they are worried about.

There are many people who feel if they hear a click on the telephone the phone must be tapped.

Education is the most important weapon we have to acquaint people as to the exposures and what people can do about eavesdropping.

We act as consultants to numerous organizations in the field of electronic security.

Certainly, my field of interest, the antisurveillance industry, is a sensitive one. While it has grown quickly in the wake of Watergate, it was not born there. It only received a shot in the arm from Watergate. And, like all rapidly growing industries, it is in need of regulation.

Machine Design Magazine warned that even when one hires agencies who specialize in countermeasures and debugging sweeps, there are a number of unscrupulous private firms who offer this service and play both sides against the espionage fence. They advise care in hiring an agency for a sweep job, to eliminate the extra risk of a double agent moving in.

The trade magazine, *Industrial Security*, also states:

"I do not doubt for a moment the existence of the obvious—the double spy. Visualize, if you will, the happy hunting ground this provides for the electronic private eye as he sets 'em up and knocks 'em down—playing both sides against the middle and each other."

With this in mind, I would certainly welcome fair regulation and licensing of firms in the antisurveil-

lance field by the proper governmental agency. I stand ready to cooperate with any efforts in this direction.

At the same time, I would like to reiterate that the antisurveillance industry is a necessary industry performing a very important task.

With all due deference to this Commission and its members, I am not convinced that legislation and even rigorous enforcement will end the 'bugging' problem. Legislation and enforcement hasn't put too much of a dent in the narcotics and numerous other problems.

Curiosity—legitimate and illegitimate—seems to be part of the human animal. And as long as this remains true, we will have illicit surveillance and a need for antisurveillance equipment and professional antisurveillance personnel.

At this point, with your permission, I'd like to demonstrate some of our equipment.

CHAIRMAN ERICKSON: That would be fine. We will be very happy to have you do that.

MR. HERSHMAN. We will give all witnesses today an opportunity to demonstrate their equipment.

CHAIRMAN ERICKSON: Go right ahead. We'd be very happy to have you do that.

MR. IEHLE: The first piece of equipment I'd like to demonstrate is our Model TA 17 telephone analyzer.

We feel that this is one of the finest pieces of telephone analyzing equipment available, if not the finest. It permits us to check any phone manufactured in the world today.

CHAIRMAN ERICKSON: Before you testify, inasmuch as you are assisting the Commission in putting together the expertise in this field—and we do appreciate it—would you tell us your background and qualifications?

MR. IEHLE: I have been involved in electronics and in countersurveillance for many years.

CHAIRMAN ERICKSON: How many years, to be exact?

MR. IEHLE: About twenty.

CHAIRMAN ERICKSON: Twenty years?

MR. IEHLE: Yes, sir.

CHAIRMAN ERICKSON: What is your educational background and training?

MR. IEHLE: My educational background is formal high school and specialized courses in electronics and special areas.

CHAIRMAN ERICKSON: I see. Where did you graduate from high school?

MR. IEHLE: Bloomfield, New Jersey.

CHAIRMAN ERICKSON: And following that, did you have further education?

MR. IEHLE: Yes, I did.

CHAIRMAN ERICKSON: And where was that?

MR. IEHLE: Some of it was at Newark College.

CHAIRMAN ERICKSON: Where? Newark College?

MR. IEHLE: Yes.

CHAIRMAN ERICKSON: And what did you study there?

MR. IEHLE: Special electronic courses.

CHAIRMAN ERICKSON: I see. And did you receive any degree?

MR. IEHLE: No, I am not degreed.

CHAIRMAN ERICKSON: How many years did you attend that college?

MR. IEHLE: About the equivalent of one year.

CHAIRMAN ERICKSON: One year's training there. And how many courses have you taken in electronics?

MR. IEHLE: I would say about seven major courses.

CHAIRMAN ERICKSON: I see.

MR. IEHLE: I have also designed and built very sophisticated audio equipment for the industry for many years.

CHAIRMAN ERICKSON: Have you obtained patents on those?

MR. IEHLE: I have a patent on one item. I do not particularly seek patents.

CHAIRMAN ERICKSON: You maintain them on a secret basis?

MR. IEHLE: I have been chief engineer and technical director for many major corporations as well.

CHAIRMAN ERICKSON: Which corporations?

MR. IEHLE: Livingston Electronics, Atlantic Recording Corporation, Ray Bender Corporation, and several others.

CHAIRMAN ERICKSON: All right. I appreciate your qualifying yourself so that we can go into your testimony.

MR. IEHLE: I am also qualified in some states and counties as an expert on documents.

CHAIRMAN ERICKSON: Thank you. Will you proceed.

MR. IEHLE: What I am doing is opening this instrument, whereby we can perform a physical search on the instrument, and as well connect our analyzer to the phone. [indicating.]

MR. HERSHMAN: Would you explain to us what you are doing while you are doing it, please.

MR. IEHLE: Yes. What I am doing is checking the lines entering into the telephone instrument, connecting the analyzer to them, to read the on-hook and off-hook voltages of the telephone and perform many other tests on the instrument.

My analyzer is now showing me that the on-hook voltage of the phone is 51.8 volts. Normal telephone voltages are 48 to 52 volts on-hook. The

off-hook voltage is shown as 5.4 volts. The normal off-hook voltages are 5 volts to 8 volts.

CHAIRMAN ERICKSON: So the device that you use to do that is a voltmeter?

MR. IEHLE: A digital voltmeter, yes, sir. And that will determine whether there are any series or parallel type devices that are loading down this particular phone line. Certain devices have telltale signs.

MR. HERSHMAN: Is this your Model TA 17?

MR. IEHLE: Yes, sir.

MR. HERSHMAN: What types of devices will that detect?

MR. IEHLE: Okay. The first test that we are looking for are parallel-type devices, be they transmitters or tape starters that are showing a voltage differential on the line, other than normal.

The second device that we are looking for on the off-hook is a series device where there is a series transmitter tap on the line.

The third device we look for is an infinity transmitter, single-tone activated. We accomplish this by feeding an audible frequency sweep to the phone, which will go through the entire spectrum. If there is such a device, it will trigger it. It will sound an alarm and show us a voltage difference on our meter.

That is accomplished semiautomatically by the instrument. If such a device were present, it would trigger it the same as I would trigger it by letting my finger go off the switch. We'd have an alarm and we'd have a difference of voltage.

The fourth test that this is performing is an all-wire combination test, where by placing the telephone in the analyzer's case, which makes an acoustical chamber, and activating an oscillator, by going through the wire combinations on a switch and listening to the earphone, it is filtered to hear only the oscillator or to hear audio leaving the phone that is not supposed to be leaving it. This will show us wire paths that are taking audio out of the room via the telephone that should not exist normally.

The last test that the instrument performs is a high-voltage pulsing which will look for switch-hook defeat mechanisms and determine whether they are present.

MR. JAMIL: Might I point out that these tests just about cover 85 per cent of the types of devices normally used in industrial espionage. There are thousands of radio and TV stores that I referred to before, selling automatic starters, parallel-type devices that start and stop a tape recorder. These are sold ostensibly with legal implications and legal applications. There is hardly a newspaper or magazine that does not carry these in some mail-

order fashion. For \$40 or \$50, together with a tape recorder, you can record automatically off the premises two sides of a telephone conversation.

This is just one of the tests that this machine will uncover.

As far as the infinity transmitter is concerned, there are numerous firms who advertise and market this device as an alarm system. There are alarm systems such as the ones that are being mailed out unsolicited that ostensibly perform the same functions as the infinity transmitter.

We feel that we have covered adequately a very large portion of the exposure of industrial espionage with this one machine.

CHAIRMAN ERICKSON: Mr. Jamil, is this a patented machine?

MR. JAMIL: May I answer that question? I am under oath.

CHAIRMAN ERICKSON: You are under oath.

MR. JAMIL: I respectfully decline to answer that question, not having prepared an answer. But I will be happy to provide an answer at a later date.

CHAIRMAN ERICKSON: Well, let's proceed with the interrogation.

MR. HERSHMAN: May I ask what a machine like that costs?

MR. JAMIL: Approximately \$2,000. It is our program to make this machine and similar type machines available to our existing and new distributors. We now have a number and we are adding on a monthly basis approximately ten distributors who will carry this machine into a businessman's office and conduct these tests on the telephone.

CHAIRMAN ERICKSON: You are going to put this in nationwide distribution?

MR. JAMIL: We are already in the process of doing that, as well as exporting it.

CHAIRMAN ERICKSON: Do you have other equipment?

MR. JAMIL: I have some other equipment.

May I add one more point. Something was said before that I think should be clarified.

I believe very much in leaning heavily on reliable equipment, but there is a certain amount of education that has to be provided. To rely on a very good machine alone is foolish and perhaps very dangerous. The value of a physical inspection by a trained technician who knows what he is looking for is about as important as having the proper equipment.

Unfortunately, there are some people who provide one and not the other.

We have another item here that we have just developed, which I am unable to demonstrate properly because of the physical conditions. But it is what we call the wiretap alert system, also using a

digital meter. It will reflect any change which would occur when series parallel, infinity transmitters, wiretaps, et cetera are used. This would be essentially the same as a TA 17 but it would operate passively on a businessman's desk, perhaps even interrupting his phone calls should a tap be placed on the line.

I'd like to point out when we talk about taps or bugs we only talk about industrial espionage. We never consider ourselves involved in any case with anything resembling court-authorized taps or court-authorized surveillance.

MR. HERSHMAN: Well, how does your equipment distinguish between illegal or court-authorized taps or bugs?

MR. JAMIL: The equipment does not distinguish between the two.

MR. HERSHMAN: Well, how do you distinguish?

MR. JAMIL: We distinguish. When we talk about countermeasure equipment and service, we are only in business to provide against industrial espionage.

CHAIRMAN ERICKSON: This new machine that you have just identified—is that available for the public at this time? Or is that in the research and development stage?

MR. JAMIL: Everything is available. Everything we are showing you today is now being shipped to the public.

CHAIRMAN ERICKSON: I see. What would be the cost of this device?

MR. JAMIL: This machine will sell for \$595. And like all our other equipment it is available through most leasing companies.

CHAIRMAN ERICKSON: Most—

MR. JAMIL: Most leasing companies.

CHAIRMAN ERICKSON: What is the name of this machine?

MR. JAMIL: It is called the wiretap alert.

CHAIRMAN ERICKSON: Do you have a model number on that?

MR. JAMIL: No.

MR. HERSHMAN: I'd like to pursue the question I asked earlier. If this equipment is available to anyone on the market—and I assume it is; you are in business to make money—how is one to distinguish again between an industrial wiretap, a marital wiretap, a business wiretap, or a court-authorized wiretap? I just don't understand, Mr. Jamil.

MR. JAMIL: I'm sorry. The machine is designed to react to changes or things that are on the telephone line that should not be there.

Our primary market that we cater to is concerned with illegal-type eavesdropping of many

types. The nature of the man behind it we have no way of discerning. I thought I answered that.

I really cannot answer for the law enforcement agency that may be legally or illegally eavesdropping. That is really your problem, not mine.

MR. HERSHMAN: The point I am trying to make is you don't run a background check on your potential customers who want to purchase these machines, do you?

MR. JAMIL: No, we don't make a background check.

MR. HERSHMAN: So very possibly a customer could be purchasing this machine to detect not an illegal wiretap but a court-authorized wiretap.

MR. JAMIL: You are saying if I were selling Chevrolet cars and someone wanted to buy a Chevrolet car for a fast getaway, yes, I'd have no way of knowing he wanted to rob a bank. If someone wants to buy this to protect against eavesdropping, we tell them the limitations and features so they can make the decision.

We normally advertise our products in trade journals, law journals, the *Wall Street Journal*, and such. We normally do not seek out those who perhaps are anxious to protect themselves against the long arm of the law.

MR. HERSHMAN: The only point I was trying to make, Mr. Jamil, is this is a piece of machinery and does not have a mind of its own. It detects all wiretaps it is designed to detect.

MR. JAMIL: That is right. A wiretap in the hands of the wrong person—yes. It would have no way of knowing that he had no right to use it.

MR. HERSHMAN: I think that this panel and the following panel are of particular importance because, obviously wiretapping and bugging is going on in the United States today, and obviously it is not going to stop tomorrow. If it goes on, then, indeed, we need equipment to lend security to those who feel their proprietary information may be stolen.

One thing we must confront, though, is the quality of the equipment, and the actual degree or scope of wiretapping and bugging in the United States today.

And Mr. Jamil, I was frankly astounded that your opening statement indicated that the scope of wiretapping and bugging in the United States is far greater than I had ever imagined.

MR. JAMIL: That is quite true.

MR. HERSHMAN: Can you tell me how you know that?

MR. JAMIL: Okay. I am glad you asked that question. I took a pencil and paper and I added up the numerous outlets for devices similar to the ones I just mentioned. If you like, I will mention them again.

There are 1,500 stores belonging to one radio chain. There are approximately 1,000 belonging to another. In addition to these two major radio chains, there perhaps are another 300 smaller radio store chains.

Every one of them carries basic items. These items are referred to as wireless intercoms, automatic tape recorder starters, telephone monitor ears, telephone broadcasting devices, et cetera.

If I were to add up these numerous stores, plus add to them the numerous mail-order companies selling the same type of devices, and in addition add the numerous importers—there is one particular importer in Commerce, New York, that had its advertisement referred to as nature's bird lover's devices. I have an article I'd be happy to make available to you.

MR. HERSHMAN: Is that a parabolic microphone you are speaking of?

MR. JAMIL: I am referring to the parabolic microphone as well as similar tape recorder starters.

Taking a pencil and paper, I add up and there are approximately 11,000 outlets for a host of little inexpensive devices, without any great sophistication. I say that this is a lot. I say that our distributors do a very, very good job of finding not one but two and three of these inexpensive devices that they come across on their travels.

I don't think that the public is paranoid. I think that the growing concern that is coming up now is of a sensible, sober businessman who recognizes that he could not afford the exposure of having his conversations and vital information picked up by somebody else.

Years ago, if you wanted to buy some bugging equipment, you'd have to spend several hundred dollars, and there were a limited number of outlets for it. Today bugs are inexpensive and they are expendable.

I hope I answered your question.

CHAIRMAN ERICKSON: You did, indeed, Mr. Jamil.

Could I ask just a few questions here?

As I understand it, you have these two pieces of equipment.

MR. JAMIL: And a few others.

CHAIRMAN ERICKSON: Oh, you have some others here with you.

MR. JAMIL: Yes.

CHAIRMAN ERICKSON: What are the other pieces?

MR. JAMIL: Phil, describe it to them.

MR. IEHLE: These are wireless detectors for bug alerts, as they are called. If you will give me a moment just to turn them on and make sure they are functioning—

MR. HERSHMAN: I wonder, could you tell us the approximate cost of this equipment?

MR. JAMIL: These range to a few hundred dollars.

MR. IEHLE: This is portable and can be carried. When in the proximity of a transmitter, which I am holding here, it will light, alerting someone to the fact a transmitter is present.

CHAIRMAN ERICKSON: In short, if I were bugged for sound or had a body mike on and came up to you and you were equipped with this detector device, you'd know that I was recording your conversation?

MR. IEHLE: Yes. The same as this notebook which has a lamp in the end of it.

CHAIRMAN ERICKSON: What is the secret behind this device?

MR. IEHLE: It is a broad-band receiver that interprets any radio transmission within its parameters into an indication which is a red light.

CHAIRMAN ERICKSON: If I walked into the room and a radio was playing, what would happen? Would the red light go on?

MR. IEHLE: Nothing. A radio is not emitting a frequency that this would see. If you had a transmitter which is a broadcasting station, it would see it and go on.

CHAIRMAN ERICKSON: If my little boy was playing with his walkie-talkie—

MR. IEHLE: It would see that as well as your citizen's band radio, your business band radio, any transmission within its parameter.

MR. JAMIL: May I point out that this is desensitized equipment. It is designed to pick up a transmitter operating at very close range. And it will filter out any walkie-talkie or radio or television. We are not interested in finding a bug a mile away. I just want to know if across the conference table my friend is carrying a transmitter.

The reason we had to get to this point is because in the old days people would carry tape recorders and bug a conversation.

CHAIRMAN ERICKSON: This is the tie-clasp microphone, things like that?

MR. JAMIL: Yes—the hidden tape recorder. We have found the astute businessman now keeps his eyes open for things like that. So the next best thing in eavesdropping—or we refer to them as 'cuties'—is to carry a small transmitter. These devices will pick up any device operating between 30 to 500 megahertz AM or FM.

CHAIRMAN ERICKSON: Do you have another device there?

MR. IEHLE: The other device, rather than being a device that is just a silent alarm—we have them in little wooden cases that are very attractive in an of-

fice and are not obtrusive. And they give a sonic alert which immediately polarizes and lets everyone know, including the man carrying the transmitter, that it has been spotted.

CHAIRMAN ERICKSON: And this would do the same thing that that little light would?

MR. IEHLE: Yes, except it tells you with an audible tone.

CHAIRMAN ERICKSON: What is the name of the one that has the red light?

MR. IEHLE: That is a bug alert, a mini-bug alert.

CHAIRMAN ERICKSON: And these are called?

MR. IEHLE: These are the—

MR. JAMIL: MW 1, 2, and 3.

CHAIRMAN ERICKSON: And what would these sell for?

MR. JAMIL: These all sell for approximately \$200 to \$250.

CHAIRMAN ERICKSON: And in connection with developing these devices, they have been put together in light of the technology that has come about regarding this sophisticated field of electronic surveillance?

MR. JAMIL: Yes, sir. We spent a number of years finding all types of radiating devices, both illicit and normal, legitimate type transmission devices.

CHAIRMAN ERICKSON: You are the president of this corporation?

MR. JAMIL: I am now the president of the corporation.

CHAIRMAN ERICKSON: And so we can fully appreciate the work that you have put into this, would you tell us what your background and training and experience is?

MR. JAMIL: Well, in 1959 I went into a business called the telephone business.

CHAIRMAN ERICKSON: The what?

MR. JAMIL: The telephone business. I was a marketer and promoter of different types of telephones for home and office.

In 1960 I discovered that people were very curious about listening to other people's telephone conversations. And inasmuch as the laws did not exist that existed in 1968, it was quite legal to manufacture, develop, advertise and market so-called bugging devices and all types of monitoring systems.

There were many that had very legitimate applications and there were some which did not have what you might call legitimate applications. We were only merchants and did a thriving business.

CHAIRMAN ERICKSON: What was the name of the company?

MR. JAMIL: Continental Telephone Supply.

In 1963 we became aware of a growing market that had existed prior to that, called a countermeasure field. Under top security requirements, we provided radiation detectors or RF detectors or bug detectors.

CHAIRMAN ERICKSON: That is the field you are in now?

MR. JAMIL: That's the field we have always been in.

CHAIRMAN ERICKSON: Let me go somewhat further into this, because what you have told us, of course, is of great significance.

What is your educational background and experience?

MR. JAMIL: I studied at the University of Oklahoma—I'm sorry, A&M College.

CHAIRMAN ERICKSON: Oklahoma A&M. Are you a graduate?

MR. JAMIL: No, sir.

CHAIRMAN ERICKSON: How long did you attend?

MR. JAMIL: A year-and-a-half.

I was eight years at Brooklyn College.

CHARMAN ERICKSON: Are you a graduate?

MR. JAMIL: No. And a year-and-a-half at Hunter College. And my main studies were in administration and marketing.

CHAIRMAN ERICKSON: In order to develop all of this rather sophisticated equipment, you, of course, had a large research and development staff?

MR. JAMIL: No. I let the large companies do the research and development. I allowed the United States Government to spend billions of dollars to develop, in the guided missile centers, the microcircuitry that I could market profitably for my bugging technique devices. I used outside engineering firms—the best, I must add—who are able to package some of the devices that I market.

I am not an engineer but I speak their language.

CHAIRMAN ERICKSON: I see. And your chief engineer is with us here today?

MR. JAMIL: That is right.

CHAIRMAN ERICKSON: Now, just one or two other questions.

These devices are devices that you and your engineer developed.

MR. JAMIL: Engineers. We use outside engineering firms to package, develop, and produce.

CHAIRMAN ERICKSON: What firms do you consult?

MR. JAMIL: Approximately dozens of firms.

CHAIRMAN ERICKSON: Can you give us some examples?

MR. JAMIL: Well, some of this would be a trade secret.

CHAIRMAN ERICKSON: Oh, I don't want to go into any trade secrets.

MR. JAMIL: I'd be happy to provide it if there is a point, at a later date.

CHAIRMAN ERICKSON: You said this equipment has some limitations, or I understand your engineer indicated that.

MR. JAMIL: All equipment has limitations. There never can be a super-duper-debugger that can catch everything. But there is something I tried to point out, that a psychological state of mind that a security director of a major corporation would employ, using the finest equipment available, a security discipline, and a training of the personnel of a company—you would at best reduce this exposure.

I'd like to meet the man who says you can eliminate eavesdropping with the use of some new equipment. It cannot be done. As a matter of fact, at this point I'd like Mr. Iehle to bring up some of the more frightening things that we know we can do nothing about, except educate people as to how those work.

CHAIRMAN ERICKSON: I'd like to hear that.

MR. JAMIL: Mr. Iehle.

MR. IEHLE: At present, in Michigan, I believe it's Senator Brown, Vasil Brown, has three bills on the floor. One of them deals with a miniature computer that is a subpiece in a central office exchange, the new electronic switch exchange.

This piece of equipment can be programmed to transfer calls or bridge calls to third, fourth, up to 12 points, in addition to the call's normal path or normal traffic.

This piece of equipment can also be programmed external of the phone company building, with use of a normal touch-tone telephone, knowing the proper code. It does not distinguish who is calling it; it just recognizes it is called.

This leaves a very treacherous area unprotected.

There are other devices that are built into the network of the telephone companies that with proper code information can verify telephone lines or listen to telephone lines as an operator would do in verifying them.

These types of devices we have no protection against.

CHAIRMAN ERICKSON: May I ask this.

In your comprehensive work in this field, did you come across any examples of industrial espionage or work that would show that there was a need for your countermeasures?

MR. IEHLE: Yes, sir.

CHAIRMAN ERICKSON: Have you ever had any experience with that?

MR. IEHLE: Yes, in many cases.

CHAIRMAN ERICKSON: Many cases? With major companies?

MR. IEHLE: With major blue-chip companies or Fortune 500 companies.

CHAIRMAN ERICKSON: Is that a fact? And would you be at liberty to disclose what companies?

MR. IEHLE: I prefer not to, sir. They can be documented but I prefer not to mention them.

CHAIRMAN ERICKSON: In connection with this, it was industrial espionage?

MR. IEHLE: It was industrial espionage.

CHAIRMAN ERICKSON: And you were able to ascertain that this was being conducted by reason of the use of your machines?

MR. IEHLE: With the use of the machines and a physical search. An analyzer and a physical search are a team. One without the other is not valid.

CHAIRMAN ERICKSON: May I ask this. You couldn't give us the names, I understand, of these companies. Can you tell us how many there are where you found this practice being conducted? Would it be over ten?

MR. IEHLE: It is difficult to tell you how many there were but if I—

CHAIRMAN ERICKSON: That you found.

MR. IEHLE: But recounting the past few months, I can say that in over seven large organizations in the past six months I have unearthed illegal devices or surreptitious listening devices.

CHAIRMAN ERICKSON: In the last six months?

MR. IEHLE: Yes.

CHAIRMAN ERICKSON: And these were all corporations that were listed in the Fortune 500 list?

MR. IEHLE: Most of them are in the Fortune 500.

CHAIRMAN ERICKSON: Were there any that were not?

MR. IEHLE: Yes, sir.

CHAIRMAN ERICKSON: Well, can you tell us how many were not on the Fortune 500 list?

MR. IEHLE: I would say three of them.

CHAIRMAN ERICKSON: So that would mean how many were on the Fortune 500 list?

MR. IEHLE: It would be four.

CHAIRMAN ERICKSON: Four?

MR. IEHLE: This is a 'guestimate,' just what I can recall off the top of my head, sir.

CHAIRMAN ERICKSON: And in the six months prior to that, did you have similar experiences?

MR. IEHLE: Yes, sir.

CHAIRMAN ERICKSON: And those companies again had equal standing?

MR. IEHLE: Yes, sir. There seems to be, from our findings, a very large amount of surreptitious listening occurring in this country.

CHAIRMAN ERICKSON: And what occurred when you disclosed the fact that these companies were being illegally surveilled?

MR. IEHLE: One corporation called in a federal agency.

CHAIRMAN ERICKSON: The Federal Bureau of Investigation?

MR. IEHLE: Yes, sir.

CHAIRMAN ERICKSON: And the Federal Bureau of Investigation was notified?

MR. IEHLE: Yes, sir.

CHAIRMAN ERICKSON: Can you tell us what state that was in?

MR. IEHLE: Are we allowed to disclose that?

MR. JAMIL: We will be happy to provide this and other information.

CHAIRMAN ERICKSON: I think that does fall within the dictates of the congressional mandate under which we are carrying out this investigation to see whether—

MR. JAMIL: May I point out at this point that there is a tendency on the part of some of our clients and the clients of our distributors to keep this information very confidential because they regard it as something to be ashamed of.

CHAIRMAN ERICKSON: Here is the whole purpose of the question, Mr. Jamil. We are not trying to violate the confidence of your client. We are just endeavoring to find out if the Federal Bureau of Investigation is doing its job.

MR. JAMIL: No man would be more delighted to capitalize on some of the more unique situations that we have run into than myself. I am a businessman. I'd love to broadcast from the roof some of the names of our customers. However, I would destroy the credibility.

CHAIRMAN ERICKSON: What area of the country? Would it be the East Coast or the West Coast?

MR. JAMIL: This is an organization having offices both in New York, New Orleans, Houston, and Chicago.

CHAIRMAN ERICKSON: It is a national organization?

MR. JAMIL: It is an organization with offices in more than one city.

CHAIRMAN ERICKSON: And as I understand it, the Federal Bureau of Investigation was notified.

MR. JAMIL: I believe it was notified.

CHAIRMAN ERICKSON: Was any other federal agency notified that you know of?

MR. JAMIL: I do not know of any others.

CHAIRMAN ERICKSON: And as I understand it, prior to this six-month period in which he said there were seven examples, four of which were on the Fortune 500 list, the previous six months produced other examples of industrial espionage; is that correct?

MR. JAMIL: Yes. But what we are doing is answering questions about our own division.

CHAIRMAN ERICKSON: I understand that. We are just trying to find out how pervasive this is.

MR. JAMIL: I will be happy to tell you we have numerous distributors who run into very similar situations as we do.

We had a recent case of a major food chain where the vice-chairman of the board could not put the hold button down on his phone. He called the phone company to claim that his phone was out of order. The telephone man opens the phone and out falls a little black box.

The telephone company just dropped dead. He said, 'I don't know who it is. Don't bother me.' and ran away.

The men immediately called their attorney who then called us.

We then were retained to check the phones of the entire company.

Well, this bizarre situation led to the discovery the next day of an additional seven very simple inexpensive wiretaps. A week later, as ordered, we came to pursue and recheck the premises.

At that point, the chairman of the board stepped in and said, "Forget about it. I don't want anyone to hear about it. Just forget about it. Here is your money. Get lost."

So it is going to be very hard for you to get the kind of documentation to verify most of these things because people sort of tend to hide the scandal.

CHAIRMAN ERICKSON: I see.

MS. SHIENTAG: We have had other testimony to that effect.

CHAIRMAN ERICKSON: Just one point here.

As I understand it, in addition to the fact that you do manufacture these devices, you also assist in determining whether there have been illegal surveillances made by using your investigative force?

MR. JAMIL: Yes. We cooperate with all our distributors and provide them with additional manpower in their physical and electronic searches throughout the United States and Canada.

CHAIRMAN ERICKSON: So you offer this service nationwide and into Canada?

MR. JAMIL: Only to our distributors.

CHAIRMAN ERICKSON: I see, to your distributors.

MR. JAMIL: Yes.

CHAIRMAN ERICKSON: What is the training of the individuals that you have to conduct these investigations for you?

MR. JAMIL: The training of the individual is as follows. He is first brought to our office where we maintain a training center. Based on his background and knowledge, we thoroughly indoctrinate him in a course so that when he is finished

he is as good as he is ever going to get, provided he is meticulous and careful and conscientious.

CHAIRMAN ERICKSON: Who teaches at this school?

MR. JAMIL: We have Mr. Iehle and a few other people.

CHAIRMAN ERICKSON: I see. And you teach as well?

MR. JAMIL: No, sir, I am only good for selling the equipment.

CHAIRMAN ERICKSON: And you sell your service.

If I headed a corporation and called for you to provide not only the equipment but the expertise to operate—

MR. JAMIL: We would locate the nearest distributor to you and offer to not only send our man down with him but make sure that he got down there as soon as possible to check and see what you needed done.

CHAIRMAN ERICKSON: Right. And you would give me a price for going through?

MR. JAMIL: Our prices are relatively standard. We charge approximately \$40 per man-hour. There are situations requiring one man-hour and there have been situations where at one point we had to put in over 100 man-hours.

CHAIRMAN ERICKSON: And the men that you would be providing to carry out this search would all be using this equipment?

MR. JAMIL: In most cases they use exclusively our equipment. We do deal with some companies or some of our distributors who have previously purchased equipment from some other noteworthy manufacturers.

CHAIRMAN ERICKSON: Have you sold any of this equipment to the Federal Bureau of Investigation?

MR. JAMIL: We believe we have. We don't know for sure. The reason I say that is they don't always identify themselves.

CHAIRMAN ERICKSON: I understand.

I believe that's all the questions I have.

Mr. Hershman.

MR. HERSHMAN: Mr. Jamil, what percentage of searches that you do reveal wiretaps or bugs? Can you give us an approximate percentage?

MR. JAMIL: I would guess that in one out of five searches we engage in we come across some kind of intrusion of privacy.

MR. HERSHMAN: One out of five?

MR. JAMIL: In one out of five of our searches.

MR. HERSHMAN: And what exactly do you do when you discover the device? Do you examine it?

MR. JAMIL: We first point it out to the owner of the premises and he makes a decision what he

wants to do with it. In many cases they have it destroyed and they ask us to forget about it.

As a matter of fact, we do not even keep files of the names and addresses of our clients.

MR. HERSHMAN: So then in many cases law enforcement is never notified?

MR. JAMIL: I don't know that. I have no way of knowing whether or not they notify law enforcement.

MR. HERSHMAN: How would it affect your business if the Commission saw fit to recommend that any bug or wiretap you discovered must be reported to law enforcement?

MR. JAMIL: Would you repeat that question, please?

MR. HERSHMAN: I'd like to know how it would affect your business if you were mandated to report any illegal finds to law enforcement?

MR. JAMIL: I have no way of knowing how it would affect the business until you actually do it. I would imagine that if we then were to be obligated to advise the customer that if we found any tap we'd have to report it, I would be inclined to believe that he would say, "Forget about it. Just sell me the equipment so I can do it myself."

And I think we would then be in danger of creating another sort of quack industry where then he would approach—with all due respect to the private investigator, you see—a private investigator who would keep his mouth shut, who may or may not have a license, who will keep everything off the record. And I think you'd take that industry and stick it underground where you have absolutely no control.

But I must admit I don't actually know what would happen until you do it.

MR. HERSHMAN: Does it ever happen that you take the device into your possession to test it?

MR. JAMIL: We never take the device off the man's premises. We have on occasion destroyed it for him on his premises and sometimes we are even allowed to remove parts of the destroyed piece to show in our so-called rogues' gallery of found devices.

MR. HERSHMAN: Earlier I questioned you concerning the scope of wiretapping and bugging in the United States and you stated you felt it was widespread because there are so many outlets for the equipment; is that correct?

MR. JAMIL: Yes. That is only one of the reasons why.

MR. HERSHMAN: It seems now we discover another reason, and that is one out of every five of your searches reveals an illegal device.

MR. JAMIL: You said illegal. I don't know. I said a device that is designed primarily to intercept his

conversation or record his phone calls or room conversations.

MR. HERSHMAN: Approximately how many searches do you do a year, Mr. Jamil? When I say 'you', I mean your company and distributors.

MR. JAMIL: That, too, is a question I'd like to answer after speaking to counsel. That may not be a question I'd like to answer at this point.

MR. HERSHMAN: Mr. Jamil, I have looked through some of your advertisements, and I am very impressed. They reflect your marketing ability. However, I am a little dismayed that none of them reflect the limitations of your equipment.

For example, I will quote from an advertisement for a 'French Disconnection' phone.

MR. JAMIL: May I interrupt?

MR. HERSHMAN: No, I'd like to quote from it.

"With the turn of a knob, the WT system automatically renders any illegal wiretap, present or future, totally inoperable."

Can any device in the world do that?

MR. JAMIL: I don't know if any device can do that, but I really can't answer for what particular piece of equipment. It was put together by people in the company before I came into control, and I don't think I am in a position to answer that question. If you want, I'd be happy to try to locate one of those instruments and have it demonstrated for you. We do not sell anything like that.

MR. HERSHMAN: This particular device was advertised under the heading of 'Communication Control Corporation.'

MR. JAMIL: How old?

MR. HERSHMAN: 1974, sir, last year.

MR. JAMIL: I'm sorry, I can't answer for what took place in 1974. I build the wiretap trap and I market the wiretap trap, and I am not saying the wiretap trap doesn't do everything it says there. And I don't know what definition you are using for illegal and what definition you are using for the taps. I was not present when these definitions were set forth.

MR. HERSHMAN: One of your recent ads says, "High profit potential in booming wiretap market. Searches out and cancels out illegal taps and bugs."

MR. JAMIL: Yes, sir.

MR. HERSHMAN: I'd like to know why you don't qualify this—and also your ad for the TA 17—qualify these to show they do not, in fact, detect all types of wiretapping and bugging.

MR. JAMIL: Well, I am not clear on exactly what your question is.

MR. HERSHMAN: It is very simple.

MR. JAMIL: Are you saying is this a high-profit business? Yes, I say it's a high profit business. Any business where you can put in hours and earn \$40

an hour is a high-profit business. My plumber charged me \$50 an hour, and that is a high-profit business, too.

MR. HERSHMAN: You showed us your bug alert. I read it detects any hidden transmitter as far away as 20 feet. Will those, indeed, detect any transmitter on the market today from a distance of 20 feet? Yes, or no.

MR. JAMIL: Any transmitter? No. In my opening statement I said there is nothing that would pick up any transmitter.

MR. HERSHMAN: But that is not what it says in your advertisements. In your advertisements it says, "It detects any hidden transmitter as far away as 20 feet." Now are you providing a false sense of security for the individuals who are going to buy this equipment?

MR. JAMIL: No, sir.

MR. HERSHMAN: Then why don't you say that this equipment is limited to the following types of devices?

MR. JAMIL: You have a very good point that the advertising part may have a tendency to be a little too general, if that is your point.

MR. HERSHMAN: That bothers me greatly, because I wonder if perhaps not only the advertisement part isn't too general but I wonder in your other advertisements—and I may quote, "As you undoubtedly know, industrial and commercial espionage has reached epidemic proportions in this country." I wonder if we are not trying to instill fear in today's society that there is so much bugging going on that this equipment is almost mandatory for every household.

MR. JAMIL: You may be absolutely right. Maybe there is no bugging going on and maybe we are all getting excited about it. All I know is that there are numerous situations where people are concerned about their privacy. We are finding bugs. There are numerous manufacturers. There are hundreds and hundreds of people in the countermeasure field.

If you are implying that the industry or the business does not exist, you may be right. That makes approximately 100 million people having dreams.

MR. HERSHMAN: I share your fears of illegal wiretapping and bugging, but I am just as fearful of overkill. And it seems to me some of your advertisements and some of your statements concerning the scope of illegal wiretapping is overkill.

I'd like to suggest, sir, that we conducted a survey where we talked to some of the most reputable debugging firms, very technically qualified—we have talked to them all over the country, and not one of them has a rate of discovery anywhere close to yours. Normal rates of discovery are less than 5

per cent. You discover one in five. Why? Are you better? Is your equipment better?

MR. JAMIL: Either my equipment is better or that is not true. However, if you like, you are invited to come along with us. We conduct with our distributors numerous sweeps on a daily basis. You are invited to come along.

MR. HERSHMAN: I accept that. I would like to not only come with you but I'd like to stay with you until you find something. And I hope that occurs before the Commission has issued its final report.

CHAIRMAN ERICKSON: Judge Pierce.

MR. PIERCE: I have no questions.

CHAIRMAN ERICKSON: Judge Shientag.

MS. SHIENTAG: No questions.

CHAIRMAN ERICKSON: Professor Blakey?

MR. BLAKEY: No questions.

CHAIRMAN ERICKSON: Chief Andersen.

MR. ANDERSEN: No questions.

CHAIRMAN ERICKSON: All right.

[Material relevant to the above discussion follows.]

TELEPHONE "BUG" DETECTOR (Analyzer Model TA 17)

The most advanced and sophisticated detection equipment developed to date, this new analyzer quickly detects wiretaps on any telephone line or instrument—any combination of wires—any interconnect or Bell system . . . regardless of the number of connectors.

Where other equipment would require hours or even days to check out a complex installation for an office or an entire building, the TA 17 completely debugs the system in minutes . . . regardless of the number of trunk lines, extensions, or complexity of the equipment.

CHECK THESE FEATURES

- Tests—without any external attachments—single line, 5-line key sets, all call directors, speaker phones, hand-free phones, logic 10 phones, logic 20 phones, plus any and all interconnect type phones or systems.
- Tests every wire combination for audio.
- Includes digital voltmeter readout.
- Tests all line pairs for triggered devices (high voltage and tone)
- Provides automatic tone sweep with automatic disconnect/alarm.
- Fast . . . takes less than 20 minutes for complete test of 5-line key set.
- Portable in handsome attaché case
- 14 x 10 x 3 inches • 20 lbs.

This advanced test set answers the need for thorough, effective, medium-priced equipment to detect clandestine wiretaps on your telephone line or instrument. The result of many years experience in designing, manufacturing and using previously available equipment, its semi-automatic operation allows over 120 individual tests to be performed on a 5-line key set in less than 20 minutes.



TESTS PERFORMED:

1. Line voltage off hook (each active line)
2. Line voltage on hook (each active line)
3. Tone Sweep (automatic) on line (each active line)
4. Line listen on hook, on line (each active line)
5. All wire listen, on hook, on line (all wires)
6. All wire listen, on hook, off line (all wires)
7. High voltage pulsing, on hook, off line (each active line)

- Works on any phone anywhere in the world.
- Undetectable by others. To prevent others in the building from knowing that the lines are under test, the tone disconnects and alarm sounds if someone picks up a phone on that line to call out or to answer an incoming call.
- Inconspicuous. Custom fitted into an unobtrusive, standard-looking case; protected by a polyfoam lining; easily portable.

TEST DETAILS

1. Line voltage off hook

This test allows the operator to measure the line voltage while the telephone is off hook (in use condition). Certain devices attached to the telephone lines or in the instrument itself alter the normal voltage and thus may be detected. The voltage is read to within .1 volt on a digital voltmeter.

2. Line voltage on hook

Similar to the off hook voltage measurement.

3. Tone Sweep

This test automatically sweeps an audio tone to activate any devices such as the infinity transmitter (harmonica bug) which may be on the line or in the telephone instrument itself. Tone disconnects from line and alarm sounds if such a device is present. To prevent others in the building from knowing that the lines are under test, the tone is removed and the alarm sounds if someone picks up a phone using that line to call out or to answer an incoming call.

4. Audio listen—all line pairs

Allows the operator to determine if the hookswitch inside the telephone has been compromised. The hookswitch normally disconnects the telephone from the outside line when the phone is put back on the cradle. Defeating the hookswitch allows the

eavesdropper to listen to the room conversation while the telephone is not in use. For this test and Test 5, the phone is placed in the TT3 carrying case with an accurate-frequency acoustic generator. A filter in the audio circuit is tuned to receive only this tone, making the test more sensitive and faster to perform.

5. All wire listen, on line

This test automatically compares each individual wire to all other possible wire combinations to detect room conversation being transmitted through the telephone wires. In the 6 button business telephone there are 1,275 combinations while in the 18 button call director there are 11,628 such combinations, in the 29 button call director there are 31,125 combinations (which takes 5 minutes). The wire being tested is identified by a numeric display. All 50 wires and the phone plug cover of a 5 line key phone are tested in less than 1 minute.

6. All wire listen, off line

A more sensitive test than on line, and provides added assurance of detecting certain techniques.

7. High Voltage pulsing

This allows the telephone instrument to be tested for hookswitch defeat methods which utilize remote triggered voltage controlled devices to pass room conversation to the eavesdropper while the telephone is "on-hook."

APPROXIMATE TIME FOR TESTS (in minutes)

Test	Single Line	5 Line Keyset	17 Line Set	29 Line Set	logic-10 system-830	logic 20 system-831
(a) Set-up Time	2.0	2.0	2.0	2.0	2.0	2.0
(b) Voltage OFF Hook	.5	.5	1.5	1.5	1.0	1.5
(c) Voltage ON Hook	.5	.5	1.0	1.5	.8	1.0
(d) Tone Sweep	2.0	10.0	34.0	48.0*	18.0	34.0
(e) Line Listen	.5	.5	1.5	2.5	1.5	1.5
(f) High Voltage	1.0	1.0	1.0	1.0	1.0	1.0
(g) All Wire audio listen ON line	.5	1.0	3.0	5.0	2.0	3.0
(h) All Wire audio listen OFF line	.5	1.0	3.0	5.0	2.0	3.0
TOTAL TIME	6.5	16.5	44.0	66.5	28.3	47.0

*If the telephone number appears on extension phones, it is only necessary to check that line once.

SPECIFICATIONS

Weight: 18 lbs.

Size: 14 x 10 x 3 Chassis (14 x 10 Face panel).

Case: Holds TA 17 and all accessories, 6 x 12 x 17 inches, cowhide exterior.

Accessories: Three (3) 5 foot, 50 lead phone cable with amphenol connectors.
One (1) Acoustic tone generator
One (1) Attache case, 6 x 12 x 17 with cable notch
One (1) Headset
One (1) Jones to clip lead cable
One (1) Operating Manual

Power Requirements: 110 or 220 Volts ac, 50 or 60 Hertz.



COMPLETE INSTRUCTION MANUAL comes with every TA 17 model.

This 28 page manual provides in easy-to-read step-by-step instructions all the information you need to be an expert on the operation of the TA 17 test set. You need no previous technical training. And CCC gives you all the professional back-up you may ever need.

Diagrams included give a clear picture of typical wiring circuits.



CONTENTS

Section I—General Description

- Purpose of Equipment
- Component Parts

Section II—Theory

- Line Voltage off Hook
- Line Voltage on Hook
- Tone Sweep
- Wire Combination Test (WCT) On Line
- Wire Combination Test (WCT) Off Line
- High Voltage Pulsing
- Listen On Line

Section III—Operating Instructions, Single-Line Telephones

- General Hook-up Instructions
- Line Voltage, Off Hook
- Line Voltage, On Hook
- Tone Sweep, On Line
- All Wire Listen, On Hook, Off Line
- High Voltage Pulsing, On Hook, Off Line

Section IV—Operation Instructions-Multiline Telephones

- General Hook-Up Instructions
- Line Voltage, Off Hook
- Line Voltage, On Hook
- Tone Sweep, On Line

- Wire Combination Test (WCT) On Hook, Off Line
- High Voltage Pulsing, On Hook, Off Line

Section V—Call Concentrators

Section VI—Test Procedure For Testing Multi-Line Phones With No Connector

- General Hook Up Instructions
- Line Voltage, On and Off Hook
- Tone Sweep
- Listen Test
- High Voltage Pulsing, On Hook, Off Line
- Wire Combination Test

Section VII—Conditions Indicating Eavesdropping Devices

- Line Voltage Off Hook
- Line Voltage On Hook
- Tone Sweep
- Wire Combination Test (WCT)
- High Voltage Pulsing

Section VIII—TA-17 Troubleshooting

- No Display
- Volts Position—Incorrect Reading
- Tone Sweep
- Amplifier
- Wire Combination Test (WCT)
- High Voltage Pulsing

OTHER EXCLUSIVE CCC TELEPHONE SECURITY EQUIPMENT & SERVICES

With purchase of any CCC Equipment you receive The Practical Guide to Wiretap & Bugging Countermeasures, an invaluable, practical reference for both laymen and professionals.



WIRETAP DEFEAT SYSTEM MARK IV

Detects and defeats illegal wiretaps which may be on your line right now . . . or which may be added at any time in the future.

The Mark IV extends the CCC security system to all four lines of a 5-button phone. It clears not just one line but any of the four lines in use.

Also knocks out telephone operated room "bugs." Easily portable for use at office or home.

BUG ALERT (EJ4)

Detects hidden transmitters up to 20 feet away. You can tell at a glance whether your conversation is being "bugged" for transmission to an outside person or recording device.

Compact, ultra-sensitive instrument gives you immediate warning when someone wearing a bugging device enters your presence. The warning is given visually and audibly, and either signal can be turned off to avoid detection.

Compact, unobtrusive, disguised as a smart cigarette box, it is portable for handy use anywhere.

TRANSMITTER DETECTOR KIT

An invaluable aid in the detection of unauthorized transmission. Model C seeks out any signal being transmitted; and Model A verifies the results. The two units are an unbeatable combination providing flexibility, accuracy and consistently high performance. Available individually or together.

WIRETAP TRAP

Revolutionary new CCC telephone unit has its own built-in wiretap defeat system.

The concealed WIRETAP TRAP automatically detects and cancels out illegal wiretaps now on your phone or lines . . . or which may be added later, knocks out any telephone operated room "bugs," and helps prevent clandestine tape recordings of your phone conversations by automatic devices or human eavesdroppers.

Also lets you know if someone is trying to eavesdrop illegally on your conversations.

- Works like a regular phone and
- Can be used on any telephone line anywhere in the world.

REPRESENTED BY:

TELEPHONE SECURITY SEMINARS

CCC regularly conducts workshop seminars on current techniques of tapping telephones or "bugging" rooms . . . and the countermeasures available today. Simple, step-by-step discussions make every point clear for both lay people and technicians alike.

ON-SITE SECURITY INSPECTIONS

Electromagnetic and radiation "sweeps" of rooms and telephone lines and instruments detect and locate taps or "bugs" in your office or home. This physical search can cover a single room or an entire building. All work done with absolute confidentiality.



COMMUNICATION CONTROL CORPORATION

441 LEXINGTON AVENUE • NEW YORK, N.Y. 10017

212/682-4637 • Cable Address: "ANTITAPS" • Telex 425313

BUG ALERT MODEL MW 2

Through an electronic breakthrough, this advanced equipment both detects and locates "bugs."

Model MW 2 detects and alerts you to the existence of a bugging device concealed on a person who enters your presence or that is planted in your room. It gives a warning by sound and light that your conversation is being transmitted to someone else or to a recording device outside the room.

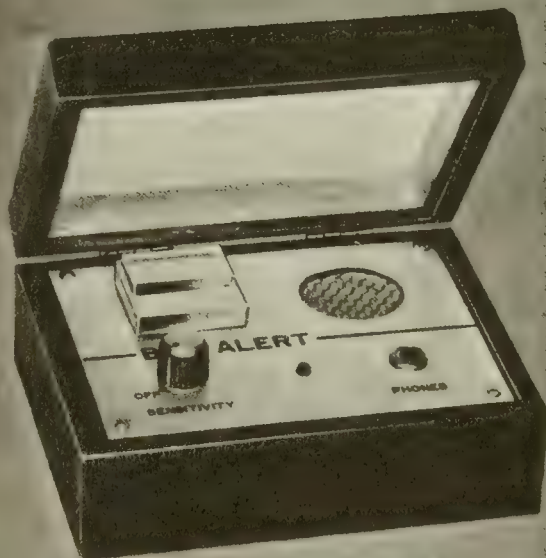
Either signal—sound or light—can be turned off at your discretion to avoid detection.

In addition to alerting you to the presence of a "bug," Model MW 2 can also be used to locate a bugging device hidden in your room. The sound signal grows louder as you get closer to the transmitter.

Inconspicuous, Model MW 2 is concealed in a small, walnut cigarette box which can be left right on your desk or placed in a drawer. It looks like a regular desk accessory.

Easily portable, you can use the unit at your office, home or on your travels—wherever you want to be certain of the privacy of your conversations.

DISTRIBUTED BY



MODEL MW 2

- Detects any hidden transmitter as far away as 20 feet.
- Includes both an audible and visual signal.
- Also usable for finding "bugs" previously hidden in a room.
- Compact, unobtrusive, portable.

MODEL MW 1. Same as Model MW 2 but without the sound signal. If you want a silent, visual signal only, order Model MW 1.



COMMUNICATION CONTROL CORPORATION

441 LEXINGTON AVENUE • NEW YORK, N.Y. 10017
212/682-4637 • Cable Address: "ANTITAPS" • Telex 425313

MR. HERSHMAN: Mr. VanDewerker, you have had years of experience with the Federal Government in the countermeasures area. You have used a variety of equipment, and I respect your knowledge.

Are you familiar with devices such as this bug alert?

MR. VANDEWERKER: Mr. Hershman, I am familiar with the technology and electrical components which are contained within the bug alert system.

CHAIRMAN ERICKSON: How effective is the bug alert?

MR. VANDEWERKER: In a given situation, it may operate to detect a modestly high-powered radio device if it is within the proximity of the transmitter, and also if the detector has the proper frequency response. But these are only a few of the electrical parameters.

MR. HERSHMAN: Would you say it is effective perhaps against only the most unsophisticated type of transmitter?

MR. VANDEWERKER: The sophistication of a transmitter may be one of the determining factors in its size, as well as a number of other parameters—for example, the modulation techniques involved, and things such as that.

Therefore, a sophisticated transmitter where the sophistication is in size only, and not in the power emitted or in the particular modulation technology of that device—the bug alert could detect it if it were in a relatively quiet RF background environment and if also the device was in some proximity close to the transmitter.

MR. HERSHMAN: Can you tell us—and I don't want to belabor your knowledge, but can you tell us what a typical bug alert would contain as far as its components are concerned?

MR. VANDEWERKER: The components in the bug alert as well as in most other field-strength measurement devices are typically a wide band or video diode solid-state device, and some amplification, which might be a small operational LSI amplifier or even just a few transistors.

The mechanism for displaying the amount of energy received is varied. It might be the simple illumination of a light as an example of the bug alert, or it might be the stimulation of a meter on the face of the equipment to indicate some relative power measurement.

But the total number of components is usually relatively few. It is a very simple device, and has been around for many, many years.

MR. HERSHMAN: Do you have any idea what these components would cost in this device?

MR. VANDEWERKER: It really depends. A crude system might cost as little as \$5. A more sophisticated detection device, sophisticated in its means of presentation of the information, might cost as much as \$50 to \$100 if it contained elaborate meters and various controls.

MR. HERSHMAN: And have you seen some of these devices for sale on today's market?

MR. VANDEWERKER: Certainly. These devices are quite popular on today's market and form the basis of the sniffer technology—

MR. HERSHMAN: What do they cost, Mr. VanDewerker, on the market?

MR. VANDEWERKER: If you buy a field-strength measurement device sold for amateur radio purposes, it might sell for \$30.00. However, if you buy a similar device with the same capability for debugging, that device might cost \$300 or \$400. There are several, however, that are sold in the \$150 range.

MR. HERSHMAN: And do you know of any bug alert that exists in the world today that will detect any hidden transmitter as far as 20 feet away?

MR. VANDEWERKER: Most certainly not. I have worked with some very sophisticated field-strength measurement devices, and there is no guarantee whatsoever. In fact, among professional circles, the field-strength measurement devices are usually a supplement to the more sophisticated professional equipment used by sweep teams.

MR. HERSHMAN: And so if I am a businessman who fears that my conversations may be overheard and I buy a bug alert, perhaps one of the Communication Control Corporation devices—although I want to mention that there are many, many bug alerts on the market aside from Mr. Jamil's product—if I buy one of these after looking at an advertisement that suggests that it is foolproof and can detect anything, and I use that knowing that my conversations then will not be overheard, I am deluding myself, aren't I?

MR. VANDEWERKER: That is correct. You might consider that a form of cosmetic security.

MR. HERSHMAN: I'd like to read from a news article in the *Daily News*, December 2, 1974, 'Rape of Privacy.' And this is an article which Communication Control Corporation distributes with some of its advertisements. It is an article solely about Communication Control Corporation. I will quote a paragraph:

"Besides their bug alert, which is placed in a desk drawer, they tout a room debugging kit which can detect a bug hidden anywhere in a room. 'Like our antiwire tap devices, it gives you two options: you find and remove the bug or leave it on to fool the bugger'."

Do you know of any room debugging kit which can detect a bug hidden anywhere in a room?

MR. VANDEWERKER: No, I do not.

MR. HERSHMAN: Any commercially available? I will limit it to that.

MR. VANDEWERKER: No, not only commercially available but I would include equipment available on a restricted basis. There are no equipments that can reliably provide that capability.

MR. HERSHMAN: That is what we are talking about, the countermeasure field, reliability and effectiveness of the equipment, and the extent to which sales reflect society's fear of electronic surveillance.

I'd like to go on to you—

MR. JAMIL: Mr. Hershman, with all due respect, I think I should add something to what you have just covered.

MR. HERSHMAN: Please.

MR. JAMIL: I think your questions to Mr. Vandewerker tended to elicit confusing answers because he spoke in more general terms than some of my advertising.

CHAIRMAN ERICKSON: Mr. Jamil, you are out of order. We will proceed to the next witness.

MR. HERSHMAN: Mr. Kaiser and Mr. Bell have been sitting there very patiently.

Mr. Kaiser, would you please explain to us your background in the field? Would you include your education? Would you tell us a little about your countermeasure equipment and show us what you have, if you have brought any with you.

MR. KAISER: Yes.

MR. HERSHMAN: And please, if you wish to address any of the subjects we have just been talking about, please do so.

MR. KAISER: Yes.

For my technical background, I don't hold very well as far as credentials; I have a B.S. in business administration from Rider College in Trenton, New Jersey. This was a secondary effort because it became obvious by the time I got ready for engineering college I was, to put it simply, beyond that point.

I have been a licensed radio amateur since I was nine years old, and this is where I get my love of electronics.

My firm has approximately 480 different products that we manufacture. When I say 'we,' I am talking about a four-people company—two assemblers, a secretary, and myself.

The electronics we manufacture are in everybody's life every day. For example, I happen to go down the list of the members of the committee, and with the exception of South Dakota, if somebody sent you a letter bomb or shoebox bomb

and you called a bomb technician, the first thing he'd take out of his case would be a bomb detector manufactured by myself.

So I am deeply involved, and I have a very, very heavy commitment to the law enforcement community.

When I got involved in manufacturing equipment, such as telephone analyzers, I developed these for agencies such as the U.S. Army at Ft. Holabird, Maryland. At that time a company called LDC, another called AEL, and Sylvania were trying to manufacture a relatively sophisticated piece of equipment. My function was to manufacture a piece of telephone analyzing equipment which would fill the development gap between the AEL and Sylvania units.

MR. HERSHMAN: Mr. Kaiser, have you sold your equipment to government agencies as well as private individuals?

MR. KAISER: As I mentioned in my opening statement, I have sold to nearly every federal agency. And I said nearly as a hedge because I cannot think of any I have not sold it to.

MR. HERSHMAN: FBI?

MR. KAISER: FBI, CIA.

MR. HERSHMAN: Did they identify themselves to you?

MR. KAISER: They sent me written purchase orders. I have been known in the community for a good many years, and the function I perform is not that of a really sophisticated engineering facility, but I do the job and try to do it as well as I can.

You are going to see an analyzer which represented in its day the best possible answer to national security problems in the area of counterintelligence. Since then it has been pretty much superseded by my honorable competitor here with his more advanced version of it. Although mine still has functions to perform.

There are three manufacturers, as far as I am aware, and they are: the F. G. Mason Company, the Dektor Company, and myself. The one you saw a while ago is manufactured by the F. G. Mason Company and I assume marketed by Mr. Jamil.

Let me run and get my analyzer.

MR. HERSHMAN: Would you please.

MR. KAISER: This, at the time it was developed, represented a combination of everything that everybody wanted in telephone analyzing equipment.

MR. HERSHMAN: What does this piece of equipment cost, Mr. Kaiser?

MR. KAISER: When I first started selling it, it sold for around \$600, and I believe its price is now around \$900, and that is because we keep putting in more developments. It is a familiar sight to some.

It is a fairly complex piece of equipment, as you can see. It represents the sum total of experience of many, many government agencies, state and federal. Their ideas are in here as well as mine. We didn't know at the time where the state of the art was going to go, so we had to make the logic flexible so as new devices came along we were prepared for them as best we could possibly be.

MR. HERSHMAN: Do you do countermeasure sweeps as well?

MR. KAISER: Very, very, very few. I try to avoid them because my love is manufacturing. That is what I do best.

MR. HERSHMAN: How many do you do a year?

MR. KAISER: I'd say three—maybe not even that many because I will go for years without doing any. Some of the more notable sweeps I have done involved Governor Mandel's phones and several other governors throughout the country. I also found our state attorney's phone tapped.

Getting back to the analyzer, it represents a limited stage in the development of countermeasure equipment, and this device does have limitations. There are no two ways about it, and in the technical report I supplied the committee, I told you basically what these limitations were and how they affect the overall scheme of things.

In my analyzer, the logic is totally programmable primarily because we hadn't reached the end of telephone tap development. Since that time, we have stopped. We stopped about two years ago, and nothing really significant has changed.

Now we have automatic analyzers like the one you saw a while ago where they can plug in the logic and don't have to rely on the intelligence or ability of the countermeasure man.

MR. HERSHMAN: Is this device capable of detecting any bug?

MR. KAISER: No.

MR. HERSHMAN: Have you ever advertised it to do so?

MR. KAISER: No. I don't think I have ever advertised it, to come down to it.

MR. HERSHMAN: I have some of your advertisements here that you send to customers who request it. I can find no statements that it detects all bugs or wiretaps, legal, illegal or otherwise.

MR. KAISER: You can't make a statement like that because it's too broad an area. And as a matter of fact, I wouldn't class that as an advertising sheet. It is really a technical description of what is in here. It tells you it has three meters, and X number of knobs for these purposes. So it is purely an information sheet and doesn't stress any capability.

But, there is one point I wanted to make, the person who uses this device has to be fairly well-

trained. And whenever you train a countermeasure specialist in the area of telephone countermeasures, you open up another Pandora's box, a tremendous one. You can't train a man how to do a countermeasure job without thoroughly training them how to do eavesdropping. And this is part of the overall problem. How do we tell this man do countermeasure work and forget the surveillance aspects of it?

I train only government agencies or government personnel—there are a few exceptions to that statement. But when a man goes out of my shop, he is just as proficient in the art of eavesdropping as he is in the art of countermeasure. And it has to be that way. How do you regulate this?

MR. HERSHMAN: So you couldn't take a man off the street, in other words, and in a week or two weeks make him a countermeasures technician, an expert?

MR. KAISER: No.

MR. HERSHMAN: Mr. Bell, could you take an individual off the street and in two weeks' time teach him how to be an expert in countermeasures—with no background whatsoever?

MR. BELL: Well, I've got to throw some qualifications in, because as I indicated in my opening statement, some significant portion of this depends upon how the equipment has been developed.

I will state some of that to you with a piece of equipment we have.

In some cases it is possible to develop a goodly amount of technology into the equipment.

Until recent years, this capability didn't exist. But we can vastly shorten the training.

Now, could we make him a countermeasures expert in two weeks? Probably not. Could we make him as proficient as the general practitioners in usual trades? Perhaps so, with an intensive two-weeks' course, and with specific equipment where a goodly amount of knowledge is designed into the equipment.

So I've got to give you a little bit of an iffy answer on that.

MR. HERSHMAN: How long is your training course, Mr. Jamil?

MR. JAMIL: As I said, it depends on the background of the individual.

MR. HERSHMAN: Your ad here says, 'No technical knowledge needed.'

Say I came to you without any technical knowledge. How long would it take me to learn to become a countermeasure expert?

MR. JAMIL: As Mr. Bell just pointed out, most of the equipment we market is on this sheet, not the old sheets you have of 1973 and 1974, and the bug alerts Mr. VanDewerker has not seen. The one demonstrated today is only on the market for a month.

Most of the equipment, as Mr. Bell pointed out—thank you for that—has all the technology built inside. You do not have to be an engineer. You do not have to be a technician. It helps if you know a little about electronics. What you don't know, in approximately 15 to 50 pages, can be absorbed.

I have a distributor who used to be a lawyer. He is very effective.

I also would like to point out there is no hocus-pocus; there is no magic to countersurveillance. It consists of hard work. It consists of physically examining every square inch of the room, physically examining and electronically examining every possible, obvious and nonobvious, place that you are going to find.

MR. HERSHMAN: While you are pointing this out, I hope you will get to the answer to my question.

MR. JAMIL: I'm sorry. What was your question?

MR. HERSHMAN: My question is: How long is your training program?

MR. JAMIL: I answered that. I said that depends on the background. We have had private investigators—

MR. HERSHMAN: One day? One week? One month? A year?

MR. JAMIL: We have people who after three hours of demonstration can operate that telephone analyzer, which I pointed out has its limitations, and these I pointed out. When the man begins to work the machine and presents himself to his client, he, too, points out the limitations.

CHAIRMAN ERICKSON: Thank you. I think you have answered the question.

MR. HERSHMAN: Mr. Bell.

MR. BELL: I guess I am qualifying experts in countermeasures. We do occasional courses of instruction at friendly foreign government level, which takes their people who are at the operating level of the country at that time, and we give them an intensive three-week course of instruction, which includes practical application with two instructors in audience at all times.

We feel that we have at that point, which is to some extent postgraduate, made them expert at the highest levels.

Now, this is expert.

Again, if we are going to consider someone—I think in my opening remarks I gave an example of the mechanic who is going to analyze the ignition with the ignition analyzer. The person who is capable of doing this does not require such extensive instruction.

And I also have made reference in my opening remarks to high, medium, and low levels of equip-

ment and proficiency to deal with those levels of threat.

So this was my problem in answering your question on a specific time.

No, not in two weeks can we take a man off the streets and make him an expert. In two weeks we probably can make him as proficient as the other trained men that we may employ, we as citizens, provided the equipment is sufficiently foolproof, sufficiently idiot proof, that the functions are essentially automatic for him.

MR. HERSHMAN: Mr. Kaiser, I am sorry for our diversion.

What pieces of equipment would your telephone analyzer be effective against?

MR. KAISER: It is going to be effective against a series device or parasite device. It will be effective against certain types of parallel parasites. It will be effective against certain single-tone harmonica transmitters and hook switch by-passes which is the process whereby we were able to monitor room conversations with the telephone on its cradle.

I am trying to look through the case here at the various components and see if I have missed any, but those are basically it.

MR. HERSHMAN: Mr. Kaiser, since you are a businessman and obviously in today's market to make money, I assume you keep an eye on competitors; is that correct? You try to keep up to date on what kinds of devices are on the market?

MR. KAISER: My opening statement relates a great deal of frustration. I have seen the government market—and I truly love the government market. That is my favorite—and I'll get to the answer. But since this well-known affair that we have talked about so openly several times occurred, the government has backed off from buying countermeasure equipment as well as surveillance equipment. And I can assure you the loss of countermeasure sales is a direct result of the government's hedging against going into this area.

So what is happening to me as a businessman is I am being forced out into the general community, and things I would have never talked about I am being forced to talk about in order to make a sale.

MR. HERSHMAN: Can you give us an example—

CHAIRMAN ERICKSON: Perhaps we can take a five minute recess at this point.

[Whereupon, a short recess was taken.]

CHAIRMAN ERICKSON: While we are waiting for the other members of the Commission to return to their seats, would you tell us what your background is in this field, Mr. Bell, what your education and training and experience is?

MR. BELL: I entered college for pre-engineering at the age of 14 and left at the age of 15 because of illness in the family. Subsequently, I was trained by the Maritime Service, was a shipboard radio officer at 17. I returned to college for two more years and entered the Army, and since have had 55 calendar months of formal education in various fields, to include advanced officer's course, Command General Staff college, as well as technical courses.

I retired from the Army military intelligence in October 1968, and in April of 1970 incorporated Dektor.

During my years in the Army, some 15 of which were in military intelligence, I worked heavily in the countermeasures field, both participating, developing, supervising the development of programs, and supervising the operations as well as other operational functions.

The staff of Dektor was selected from the several government agencies involved in this, with representation from DOD, National Security Agency, and CIA—selected personnel who had extensive developmental, instructional and operational background in countermeasures.

We have on our staff former instructors from the training programs in this area from both the Army intelligence school and CIA's advanced training program.

At the present time, something in excess of 50 per cent of our activity is devoted to countermeasures. The remaining less than 50 per cent is in psychological stress evaluator which is another of our developments.

We perform, in addition to development of countermeasures material, extensive threat research, as threat models for the countermeasures equipment. And as a consequence, we are operating at the very highest levels, the most sophisticated levels, in this area.

CHAIRMAN ERICKSON: Mr. Hershman.

MR. HERSHMAN: I think this would be a good time since we are a bit over, Mr. Bell, if you would show us some of your equipment, please.

MR. BELL: Okay. Since we have been dealing in each case with telephone analyzers, I'd like to show you briefly and discuss what Mr. Kaiser has referred to as the next generation of telephone analyzers.

We have three telephone analyzers.

MR. HERSHMAN: Could you tilt that a bit, if it is possible?

MR. BELL: We have three different levels of comprehension.

Telephone analysis is broken down into two parts. One part is referred to as on-line test, which is the attempt by voltage and current measurement

to detect additions to the telephone line which may have been used for tapping telephone conversations, as well as one type of bugging device, which is the infinity transmitter.

I will disagree with Mr. Jamil in that multitone infinity transmitters are undetectable. We have developed a device which we call a Polytonic sweep which is a mathematical array to permit us to hit two or more frequencies simultaneously.

The assurance that this is going to occur is quite high, considering the constraints that are placed upon the manufacturer of the infinity transmitter. The theoretical assurance that it will be done in each case cannot be given. But within the limitations of finding the single-tone infinity transmitter, the Polytonic sweep will find the multitone. This is incorporated at the present in this telephone analyzer.

However, most of the on-line checks are simply state-of-the-art checks by a piece of equipment that has ability to read voltage and current. The problem here is that while perhaps 95 per cent of the devices that are used in quantity can be detected by this means, there are types of devices that cannot. A high impedance amplifier tap, a high impedance transmitter in parallel, a tap back at the exchange—none of these things can be detected technically by any means.

MR. HERSHMAN: Have you ever suggested in an advertisement that this piece of equipment could detect any bug or wiretap?

MR. BELL: No.

MR. HERSHMAN: Do you advertise?

MR. BELL: Oh, yes; yes.

MR. HERSHMAN: I have some of your advertisements here and I see nowhere in them where you suggest that it can detect all devices. As a matter of fact, I see you give some exceptions in your advertisement of what it will not detect.

MR. BELL: That is right; that is correct.

MR. HERSHMAN: What does this machine cost, Mr. Bell?

MR. BELL: This costs \$5,200. There is a companion unit that goes with it for sequencing—and I'd like to say a word more about both of these.

MR. HERSHMAN: Certainly.

MR. BELL: In the second part of telephone analysis, which is the true telephone analysis, the object is to examine every permutation of the conductors coming from the telephone to determine if any interconnections of any sort have been made that could permit the transfer of audio from the telephone in a hung-up condition.

The first look at the telephone is primarily to determine if telephone calls could be intercepted. This is tapping. The second is to determine if the telephone has been converted to a room bug.

And there are quite a number of modifications that can be made to the telephone to accomplish this.

What we have done in approach is, rather than attempt to go and identify or program for the detection of this device or that device or that device, we have designed equipment which down to extremely close tolerances will detect any addition to any component.

Now, this is a little different. We don't require that the thing even be an operating bug. The first thing we want to know is: Has anything been added to it?

Then in the next phase of the operation, we will go into the identification and resolution.

And this is where the digital circuitry is involved in this model.

In lower-price models which go down to \$1,060 for the lowest priced one, we will have the same detection capability. In other words, we can detect the addition of any capacitance between any two conductors as low as 200 millionths of a millionth of a farad, which is unusable for audio interception purposes; as high as 5 million ohms, which is equally unusable for interception purposes, with voltage fire devices up to 6,000 volts, which is a higher voltage than the bugger can use because of his losses as a result of line capacitance.

Now, what we can do with this at the present time—we have demonstrated to this. In answer to another question which is coming up, yes, we sell to the federal agencies. We sell to essentially all of them.

MR. HERSHMAN: How do you know that?

MR. BELL: In most cases it is with purchase orders, and we bring in men and train them along with the equipment. I think we have had one or two cases where the purchase has been made through the procurement officer at Fort Meade but by and large we operate right directly with the agencies.

Okay. So this is our approach to the telephone analysis.

It has been a little over five years in the development, starting from what state of the art was at that time, and with personnel who were thoroughly trained and completely conversant in the area. And we are quite proud of it.

MR. HERSHMAN: Mr. Bell, what is the state of the countermeasure market today?

MR. BELL: Dismal.

MR. HERSHMAN: Do we have any idea how many countermeasure manufacturers or distributors there are in the country? Could you hazard a guess?

MR. BELL: I really couldn't. What happened in 1968 is a lot of people who were very small opera-

tors in the bugging and wiretapping manufacturing business—these are referred to as basement operations and 'mom and pop' operations, and so forth, and some of them quite clever—many of them swung over to attempt to earn their livelihood from the other side of it and avoid the illegality of operating under the Omnibus Crime Bill. And there are quite a number of these.

I think I mentioned to you that we had followed up on an ad in one of the Washington papers for having your telephone cleared.

MR. HERSHMAN: I am glad you brought that up. I understand you have a tape recording with you today.

MR. BELL: Yes.

MR. HERSHMAN: Could you get that?

MR. BELL: Sure.

MR. HERSHMAN: Let me explain to the Commission. During the last few weeks an ad has run in the *Washington Post* under personal advertisements, and the ad states, 'Have your phone debugged,' and gives a telephone number.

A member of Mr. Bell's firm called that number and recorded the conversation with the person offering this debugging service.

MR. BELL: This seems like a tangent but I am leading in from this to answer your question about some of the small operations and perhaps some of the security hazards that arise as a result of them. I will give you an opinion once you have heard this.

Actually, the telephone call is rather long. I think in the interests of time—I will leave the tapes with the Commission. There were two telephone calls made by two different people, but I think from the first three or four minutes of this we can get the gist of what this operation is.

I will also give you an opinion of the equipment that is in use on this, the cost of it, and probably who manufactures it.

MR. HERSHMAN: Mr. Bell, would you kindly furnish the Commission with a copy of that tape so that we may make a transcript for our records?

MR. BELL: You may have these.

MR. HERSHMAN: Thank you.

MR. BELL: I have no further use for them.

If you can't hear this, we can play it into the microphone.

[Whereupon, a portion of the tap was played as follows.]

'Q I am calling in regard to your advertisement in the *Washington Post*.

'A Un-huh.

'Q And I'd like to speak to someone about it, please.

'A The bugging?

'Q Yes.

'A Just a moment.

[Pause.]

'A Hello, sir.

'Q Yes.

'A Could I call you back?

'Q No, I'd rather call back myself.

'A Call me back on 2357.

'Q Who shall I call for?

'A Vincent, V-i-n-c-e-n-t.

'Q Mr. Vincent?

'A Yes.

'Q Thank you.

'A Bye-bye.

'Q Mr. Vincent, please.

'A He just walked in the door. In a few minutes he will be right with you.

'Q Thank you.

'A (New voice). Can I help you, please?

'Q Mr. Vincent, please.

'A This is Miss Vincent.

'Q I'm sorry, they gave me Mr. Vincent.

'A That's okay.

'Q A little discrimination going on there. I'm calling in regard to your ad that was in the *Washington Post* on bugged phones and so forth, that are bugged. And I'd like to get a little information on it, if I may.

'A Yes, certainly.

'Q As far as—naturally, how much does it cost?

'A Well, it depends on how many lines are on the phone and how often you want it checked, if you want it just checked once.

'Q Well, I would feel much better if it is done more than that. What do you recommend?

'A Well, you know it would depend on the circumstances. It could be done once a day; it could be done once a week, or however often you'd want it checked. I would think that—

'Q Well, it is a business phone, and it is one of these that has—let's see—six buttons. One's a hold button, I guess, so it's got five buttons, and we also have an intercom. So I guess it's four lines.

'A On the same number?

'Q Yes.

'A And the others are like rotary?

'Q What do you mean by rotary?

'A If your main number is 546-3000 you might have 01, 02, and so on.

'Q That is the way it is.

'A Then it would just have to be the one number that is checked because if there is anything on the phone, it would show up regardless of which one it would be on, you see.

'Q I see.

'A Now, it is the phone that you are primarily concerned with? Are you primarily concerned with anything in the room, microphones?

'Q No, just because of business and things that have been happening here lately and things I have been discussing over the phone I have been hearing other places.

'A Is that a fact?

'Q From time to time, and it may be coincidence. But I know there has been a lot of talk here lately about things like this, and of course, I saw the ad in the paper.

'A Would you like me to come out and talk to you about this, or do you want me to give you our rates for a daily check?

'Q Well, a daily—is that someone physically coming out?

'A No, we don't have to come out.

'Q How do you do this?

'A We have equipment.

'Q Right. I understand that.

'A Are you in Washington?

'Q Yes, I am in Washington.

'A No, we have equipment that can determine this. Now, if this is something the government is doing we don't have any way of finding that out.

'Q What do you mean?

'A In other words, let's say the FBI or CIA or the Pentagon or somebody is getting into your phone from some source other than your phone itself, other than the basement terminal, or other than the telephone pole. Those are the three things that would show up.

'Q I see; I see. No matter what they were doing? In other words, I could feel safe that once it is checked, if it was anything like you say, the pole or the phone or in the basement that it would show up?

'A Yes, yes, definitely. I will tell you what you might consider doing is having us check it. Our first check is nominal, and I have inquired other places and the charges are exorbitant. We charge \$25 for the first check. We don't have to come out. But if there is a microphone in the room now this won't show up. This will pick up anything that is on your phone.

'Q But in other words, you don't even have to come out here—

'A No, we don't.

'Q —to do the check?

'A I don't have to come out to find out if there is anything on it. Now, if something is on it, then we have to come out to find it.

'Q I understand that.

'A See?

'Q Okay. What do you need, then? Just the phone number?

'A I need the phone number, and I need to have you not answer the phone. For instance, we could plan to do this at a time when—'

MR. BELL: This goes on.

MR. HERSHMAN: I'd like to ask a few questions. She was suggesting she needn't come to your office to check your phone but do it from her office?

MR. BELL: That is right.

MR. HERSHMAN: And she was going to charge you \$25 to check one line, and she'd offer you this service on a daily basis?

MR. BELL: That is right.

MR. HERSHMAN: So you can come in in the morning and be sure your phone is clean?

MR. BELL: Yes.

MR. BLAKEY: Did she want you to send her money?

MR. BELL: Oh, yes.

[Laughter.]

MR. HERSHMAN: And you'd just pick a time of day and not answer the phone while it rang, is that right?

MR. BELL: I think I can infer what piece of equipment she is using.

MR. HERSHMAN: If she is using any piece of equipment. How do we know?

MR. BELL: I think she is. You see, in the three categories I brought out, I am not certain that she isn't in the 'sincere but ineffective' category. In our conversations—this was Bob Wingfield from our offices, and the other tape, after listening to the first, was done by Mr. Pelicano, an associate of ours from Chicago.

We really didn't determine that she was a charlatan in the absolute sense. I don't know how she got involved in this thing.

Incidentally, this is Mary Vincent, I believe, and the company is Aaron's Business Services, which is a telephone answering service.

MR. HERSHMAN: Here in Washington?

MR. BELL: Yes; not too far from here. Apparently, as nearly as we can determine, they have two pieces of equipment, both of which may have been put out by R. B. Clifton in Miami.

MR. HERSHMAN: That is a Miami manufacturer.

MR. BELL: Yes. The one she was talking about here for clearing the telephone lines, from little bits and pieces that she mentioned, would seem to indicate a device put out by Clifton which is called the phone sweep.

MR. HERSHMAN: Excuse me. For the benefit of the Commissioners, the tone sweep—

MR. BELL: The phone sweep.

MR. HERSHMAN: It's Exhibit No. 13 in our book, the last page.

MR. BELL: This one here.

MR. HERSHMAN: I have supplied to the Commissioners a copy of that, and it is the last page of Exhibit No. 13.

MR. BELL: That is what is being used there. The fallacies with this piece of equipment are two: First, in sending this phone sweep through the phone system, the amplitude of the signal is vastly limited which doesn't give you as good a chance of getting it as if you are going across the phone line with higher voltage. This is a product of the curve of the filter which is associated with the infinity transmitter. The only thing it could conceivably pick up is an infinity transmitter. It could not get phone tap devices.

MR. HERSHMAN: Could it pick up an infinity transmitter?

MR. BELL: Perhaps at 30 percent effectiveness. I am going to reduce it to 50 per cent effectiveness based on the fact it has to go through the exchange rather than being on the line. And I am going to have to take 40 per cent of the 50 per cent away because that is the duration of the ring signal. When the ring signal is hitting that device, it isn't getting her signal coming through the exchange. So I would estimate a 30 per cent factor.

MR. HERSHMAN: Mr. Bell, what is to prevent me from putting an ad in the paper of the same nature, never purchasing a piece of equipment, and having you sit there and listening to rings all day long, and have you sending me checks?

MR. BELL: Not a thing. The second piece of her equity involved a regenerative broad-band device which possibly also—because Clifton does make one of those—could have come from Clifton as well. She mentioned the equipment came in from Florida, and this is one of the things indicated, in addition to the advertising sheets from Clifton, that it may have been.

MR. HERSHMAN: Mr. Bell, you, Mr. Kaiser, and Mr. Jamil have shown us some very sophisticated equipment today. Does this typically represent what is on the market?

MR. BELL: No, I don't think so. A large part of the problem—some of the problem, of course, as Mr. Jamil indicated, is the money maker, the individual who doesn't care really what he does or what is the level of performance, as long as he gets his pay.

MR. HERSHMAN: How do we stop that?

MR. BELL: The others include people who may plant devices. Perhaps another category of these is the individual who will find a device that they have brought with them to show the client how effective they are. Frequently these are people who realize they are ineffective, and it is something of a con operation, of course.

MR. HERSHMAN: Would you prefer to see licensing in the manufacturing area or the use area?

MR. BELL: Both.

MR. HERSHMAN: How effective do you think licensing would be in governing manufacturers of this equipment?

MR. BELL: I think this could be quite effective because if we were to attack this from a really dynamic performance standards standpoint and require, just as we do on this pack of cigarettes, that a warning be applied in advertising, in bids, in solicitations, which are based upon the equipment, of the capabilities or the limitations of the equipment, then I think this could be extremely effective.

MR. HERSHMAN: You mean one phase of the licensing would require that any advertisements would have to specify—

MR. BELL: —the limitations of the equipment.

MR. HERSHMAN: What it is effective against.

MR. BELL: You see, as a manufacturer, I probably shouldn't be making a recommendation of this sort. I am willing to do it because I am willing to live under it. If our equipment does not meet certain standards, I both have the facilities and I am willing to go back into the lab to make it do it.

Ultimately, I would like to see us turn out the absolutely best kind of equipment in the world, and we are dedicated to doing this, and I have no qualms about being evaluated from this standpoint.

MR. HERSHMAN: Who would you recommend to control this licensing?

MR. BELL: The equipment manufacturers' licensing and the establishment of standards and so forth, I would like to see, if it could be arranged, in one of the federal agencies which is involved in this sort of thing at the Federal Government level already. And I would like to see this because I have seen the problems that have come up with Underwriters Laboratories establishing standards for the alarm industry. We have never yet after 20 years and perhaps hundreds of attempts gotten acceptable alarm equipment standards.

That is one of the reasons we are trying to make, instead of standard technological specifications, functional standards. So I would like to see this go into one of the agencies which is involved at the present time in evaluating equipment of this sort for their own purposes, where the expertise is located, where the threat analysis is located, where the common sense is located.

MR. HERSHMAN: And who would you recommend to determine the standards for this type of equipment?

MR. BELL: I think the standards possibly could best be accomplished by a joint government-industry task force. I think it could, because in some

cases there would have to be different points of view in the civilian area from some of those in government, because cost is going to be a factor in this to make it useful to the ultimate consumer.

But I would like to see very strong, very expert government participation in the establishment of the standards as well.

We have several agencies who are and have been for many years involved in just this sort of thing for the purposes of the Federal Government.

I think it is perhaps time that we used some of this for the protection of the larger scope of the people out here that are not government agencies.

MR. HERSHMAN: Can licensing of manufacturers work without licensing of users?

MR. BELL: It can work up to a point. As Mr. Jamil again pointed out, there are two factors. And although I am not sure he said it exactly this way, each of them stands alone.

We could require that equipment meet certain specifications or meet certain standards or at the very least that the standards be stated and the performance characteristics be advertised; that the limitations be specified. And we could greatly enhance this whole problem in that manner alone.

Now, we could add to it somewhat if we could have a reasonable licensing law. And I think the 3,000 hours that was mentioned by an earlier speaker here may be arbitrary. I think ultimately we are interested in what level of proficiency the individual exists at. And we have a mechanism for this already, mechanically and physically, which is the FCC with amateur radio licenses. I think the procedure should be essentially the same. The testing locations are already there. The procedure here is to determine what an individual should know in order to be able to advertise as a Class A, Class B, Class C or D countermeasures specialist, be examined for this, have it specified and have it controlled on that basis.

MR. HERSHMAN: Mr. Kaiser, would you basically agree with what Mr. Bell has put forth?

MR. KAISER: I think what he has to say is very sound. I am just trying to again, from a very, very small business standpoint, figure how this is going to hamper or accelerate my business. It is a very difficult thing. I have been totally frustrated by the Omnibus Crime Bill. It just seems that business has been taken away from me by the bill itself, primarily through nonenforcement.

So I am a little skeptical about licensing of either one of these categories. If I had to lean any way, I would want to license both of them, and I think the suggestion made yesterday, I believe by Mr. Holcomb, to have ATF handle the licensing, would be a valid solution.

MR. HERSHMAN: Yesterday Mr. Holcomb also mentioned that he interpreted the law to read that he is allowed to demonstrate and display, allowed to inventory, and allowed to have sales personnel carry around devices.

MR. KAISER: This is one of the problems. In dealing with the agencies that we deal with, of all types, starting with the CIA and working on down, they are very hesitant about putting anything in writing. But when I get a call from the office of the Attorney General of the United States and he says, "Mr. Kaiser, do not stockpile equipment," and I say, "How much is a stockpile?" and he says, "That is for you to determine," I believe the man is threatening me with prosecution if I stockpile.

MR. HERSHMAN: How do you feel about someone else doing it in the same business?

MR. KAISER: As I mentioned in my opening statement, I took this to the Justice Department and never saw such a run-around in my life. I have been fighting this for six years and am no closer to a solution.

MR. HERSHMAN: You told the Justice Department there was a manufacturer who was apparently violating the law?

MR. KAISER: I have cited in the years I have been in this business about 25 of what I consider direct violations—open advertising in newspapers—that is specifically prohibited under the Omnibus Bill. And absolutely nothing has been done. And they were so upset they said, "Don't try to use us as your personal attorney. You are trying to limit competition."

I said, "No way. All I am trying to do is get the guidelines set up so we can operate smoothly."

This is what I meant about being so frustrated in my opening statement. I'd definitely like something to be done because it has just gotten out of hand now.

MR. HERSHMAN: Which brings me to another point. How do you efficiently and effectively teach countermeasure services to individuals if you can't possess an offensive device?

MR. KAISER: Right. There is no way you can. And the way I solve the problem, since there are very, very large number of federal, state and local agencies that buy equipment from me, the probability of my having a device in my possession when a man is there to be taught countermeasures is very good. I meet the law because even though I am in possession, I am under contract. And I use that device to demonstrate, and then it goes out the door, and that's that.

So that is how I solve the problem.

But there definitely should be licensing to provide devices for countermeasure specialists.

But again, in the process of teaching, you don't need any equipment in telephone countermeasures. Just moving a wire from one hook switch contact to another solves the problem. When the wire is hooked up one way it is a bug, and when you put it back another way it is not a bug.

MR. HERSHMAN: Mr. VanDewerker, I believe you have some comments.

MR. VANDEWERKER: Yes, thank you.

I would like to, along with my associates here at the panel, submit an opening statement at a later time, a brief statement.

[The prepared statement of John S. VanDewerker follows.]

STATEMENT OF JOHN S. VANDEWERKER,
GENERAL MANAGER,
ASHBY & ASSOCIATES-SYSTEMS DIVISION

Mr. Chairman and Members of the Commission. My name is John VanDewerker; I am the manager of all security activities of Ashby & Associates.

The firm is seven years old and was formed to represent client interests in Washington. Ashby & Associates is actively engaged in this representation function with offices in Washington and Los Angeles as well as having associates in many major cities of the world.

Approximately four years ago the Systems Division was established to offer electronic surveillance countermeasures products and services to the foreign and domestic government, law enforcement, and private sectors. The services provided included technical consultation, engineering design and evaluation, security inspection, and training. We feel that our business is the premier firm in electronic surveillance countermeasures because all of our personnel are professionally trained in technical disciplines and experienced in rendering services based upon training received in the federal intelligence community. For example, I am an electrical engineer and have seven years experience in electronic security work with the federal community in development and use of electronic surveillance, countermeasures, and navigation and tracking equipment.

It has been an honor for Ashby & Associates to serve as a contractor to this Commission in the preparation of a report regarding the state of the art and science of electronic surveillance. Hopefully, this endeavor will afford the Commission, the Congress, and ultimately the public a better realization of this subject that is too frequently misunderstood. While it is premature to express our recommendations resulting from this study, we have documented findings and reached numerous conclusions that necessitate some address during evaluation of electronic surveillance legislation. We have studied the full spectrum of audio eavesdropping technology including telephone surveillance systems, microphones, radio transmitters, optical transmitters, and recording devices. We have also explored in depth the countermeasures to audio eavesdropping including the devices and organizations that perform audio countermeasures services. Extensive review has been made of interception of non-audio information including eavesdropping upon computer data and bulk communication transmissions, other information processing equipment, and machine emanations. An evaluation of electronic aids to physical surveillance has been conducted and an assessment of future electronic surveillance systems and technology has been completed.

Finally, let me thank the Commission for the privilege of serving here today and for the opportunity to assist this important work as a consultant.

MR. VANDEWERKER: Generally, during the course of the preparation of the state of the art study, one observation I made in talking with law enforcement agencies across the country was that perhaps one of the reasons for the enforcement of the laws as written is that the law enforcement organizations themselves do not understand the art of audio penetration. And frequently, for example, in Los Angeles recently small devices were found and the law enforcement organization called in at that time was really unprepared on how to handle this particular situation. They did not know how to verify it was a surveillance device. They did not know really who to turn to, who to talk to. I think they were reluctant to talk to the telephone company or the FBI.

So one of the recommendations I'd like to add to Mr. Bell's list, which I agree with, is that some guidelines be established to support police organizations to assist them in their preparation and evaluation and handling of suspected electronic penetration devices.

In addition, we have generally talked about here today several items, but the one most frequently discussed was the infinity transmitter. And I'd like to add that to turn on or activate the infinity device in some cases can be very difficult with the multitone equipments that are coming on the market—very difficult to stimulate into operation. They are, however, easy to detect, and if a person suspects that an infinity device is on his telephone line, he might procure a \$10 voltmeter and measure the voltage on his telephone when it is not in use to determine whether the line is in use or not in use and get away from some of the more costly methods.

In the case of the multi-line office phone, the push button light will turn on, indicating it is being used, as it does when you are using the phone in a normal situation.

MR. BLAKEY: May I clarify what you said?

MR. VANDEWERKER: Yes.

MR. BLAKEY: You mean it would be possible to adapt the normal push-button phone so that the light will come on when the infinity transmitter came on?

MR. VANDEWERKER: In the normal push-button office phone, when you pick up the handset, the light comes on indicating that the line is in use. Having a light turn on when the telephone line is used by the infinity device would also be possible.

MR. BLAKEY: And it would be just as simple.

MR. VANDEWERKER: It would be just as simple as measuring line voltage with a voltmeter for a single-line phone. This is all that is necessary to

determine any infinity device that is activated on the line. This does not stimulate or activate the device. But in a situation where the voltmeter would be connected to the line permanently, if for some reason the line is used, as you'd see an obvious change of line voltage.

I'd also like to comment about the level of automation, coming to the various analyses equipment.

This government as well as other governments, I'm sure, have spent a great deal of funds trying to automate countermeasure equipment.

However, they have since nearly decided this is a fruitless endeavor because of the need for the human intervention in the process of countermeasures. The interpretation and assessment of a piece of equipment is essential—at least they feel it is necessary at a higher level of sophisticated countermeasures. And for this reason, many groups are very hesitant to use automated systems for their countermeasure activities and insist on using types of equipment that are manually operated to some extent, and have continuous human intervention.

Finally, I'd like to also point out that telephone countermeasure is certainly only one of a multitude of equipments that are required by professional sweep organizations. The telephone represents certainly a likely candidate for the placement a device. However power lines and other communications lines also have to be assessed during a countermeasures inspection. And this requires as a minimum countersurveillance radio receivers designed for this purpose, to cover the required radio frequencies and the telephone analysis equipment described here today. It also might require various non-linear device detection and extra modulation analysis equipment.

This is why the cost of the whole countermeasures package might easily run to \$20,000.

As an adjunct, there are field-strength meters and metal detectors.

MR. BLAKEY: Thank you.

CHAIRMAN ERICKSON: Judge Pierce.

MR. PIERCE: No questions.

CHAIRMAN ERICKSON: Chief Andersen.

MR. ANDERSEN: No questions.

CHAIRMAN ERICKSON: Judge Shientag.

MS. SHIENTAG: No questions.

CHAIRMAN ERICKSON: Mr. Blakey.

MR. BLAKEY: There was one thing, Mr. Jamil, in your earlier testimony that I was not clear on. Whatever happened to Continental Telephone?

MR. JAMIL: Went out of business in 1970.

MR. BLAKEY: Why?

MR. JAMIL: I don't know. I left in 1969.

MR. BLAKEY: Thank you.

CHAIRMAN ERICKSON: Mr. Jamil, prior to your leaving Continental, what type of device did they manufacture?

MR. JAMIL: Prior to 1968, we manufactured surveillance and countermeasure equipment.

CHAIRMAN ERICKSON: And after the advent of the Omnibus Crime Control Bill, you had to give up the manufacture of surveillance equipment?

MR. JAMIL: We reluctantly destroyed over a quarter of a million dollars of surveillance equip-

ment and decided to operate completely out of that field.

CHAIRMAN ERICKSON: I see. Thank you very much.

Gentlemen, we appreciate your time and devotion to the effort to make the Commission aware of the equipment that is in use today. Thank you again for appearing.

[Material relevant to the above discussion follows.]

DAILY NEWS

NEW YORK'S PICTURE NEWSPAPER ©

New York, N.Y. 10017, Monday, December 2, 1974*

ONLY HUMAN

Rape of Privacy

By SIDNEY FIELDS

Paula Lippin tells the story of the company president who greeted his visitor, opened his desk drawer, then terminated the visit before it started because the flashing light on the "Bug Alert" in his drawer warned him that the cigaret lighter the visitor placed on his desk after lighting a cigaret was probably bugged, and the brief case he'd tossed on a chair probably held a tape recorder.

There's a lot more rape of American privacy in business and the home than there is of women," Paula was saying in her office the other day.

Paula is vice president of Communication Control, a small New York outfit that's big in researching, developing and selling ingenious devices to defeat bugging and wiretapping. That's a strange vocation for a 40-year-old divorcee with three teenage children who once taught health and physical education in the city's high schools. She left teaching after she had her children to do research and marketing for a Wall Street broker. Paula was asked to find out how information on a special stock leaked out of the office. She knew nothing about it, so she went to the experts, found a man named Bob Soames, who quickly discovered that the chief researcher's phone was tapped.

Bob Soames intrigued her with an account of how widespread electronic eavesdropping had become. He said that Hazel Bishop cosmetics had lost about \$30 million in one year because its trade secrets were lifted through wiretaps, and the late Lewis Rosenstiel of Schenley Industries had experts trace the leaks of valuable confidential information to a bug in his Miami home and a tap under the roof of his office building which led directly to his private phone. After dozens of other such brazen taps and bugs came to light the federal government made it illegal to manufacture, sell, purchase, possess or use electronic eavesdropping devices except by law enforcement bodies, and then only by a court order. But it still goes on illegally.

Paula told Bob that it would be a great thing to develop devices to stop uninvited eavesdropping. He agreed, got a friend, Charles Bonner to back them, and they started Communication Controls in 1972.

"Bob Soames became our brain wave," said Paula.

Every week they ship out up to 50 of them all over the U.S. One is a gilded French phone with an ingenious wire tap trap inside the box. They call it the French Disconnection. Another is the Line Tap Defeat System, which determines what kind of tap is being used, where it's located, and knocks it out.

The LTD systems are used by some 70 police departments and district attorneys in the U.S., including New York, Boston, Atlanta, Connecticut and Union County, N.J. A big city mayor had one installed in his office, and a week later his police commissioner asked for one.

"We had to tell him that the mayor already



Paula Lippin—Uninvited eavesdroppers?

had one," Paula said, "and we had to inform the mayor that the police commissioner wanted one. It seems they were feeding with each other."

One of Paula's engineers, Kevin McAleavy, 24, developed the Wire Trap, a small box which is linked to the telephone and flashes a red light when the line is being tapped. By hitting a tiny switch the light is off and the tap is knocked out, if the user wants to send out false information he leaves the light on.

"We'll be selling it in a few months," said Paula. "It should be useful for lawyers, doctors, and business executives for home use."

Her other clients include dress designers, companies developing new products, a national moving van outfit, others who have secrets to protect, and even husbands and wives who check up on each other.

"If you think a telephone is a private instrument, forget it," Paula said.

Besides their Bug Alert, which is placed in a desk drawer, they tout a Room Debugging kit which can detect a bug hidden anywhere in a room. "Like our anti-wire tap devices it gives you two options," Paula said. "You find and remove the bug or leave it on to fool the bugged."

Bob Soames, Kevin McAleavy and Paula are still amazed at all the places they find bugs: in chair upholstery and electrical outlets, under carpets and above dropped ceilings, the base of a stapler, behind wall panels, the pen of a desk set, in tie pins, cuff links and even teeth caps.

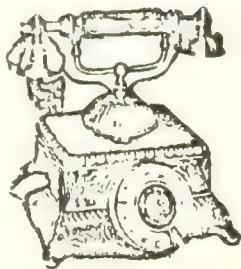
"One man sent his friendly competitor a handsome little radio as a gift," Paula said. "He plugged it in and put it on his desk. Whether he plays it or not everything he says is being heard by the sender. There's a \$5.95 transmitter inside. Any kid can buy one."

DEFIES TAPPING new phone unit offered

Something for the man who has everything ... everything to lose, that is, if his phone is being tapped. In the aftermath of Watergate, there breathes not a Chairman of the Board who doesn't worry about wiretappers, company says. Now the "ultimate weapon" has been made available to the concerned executive, according to manufacturer. Its name: "The French Disconnection." Its game: It's an elegant antique telephone, burnished gold in color, stylish in design. But, it has a secret: it is absolutely 100% safe from illegal wiretappers and telephone "buggers," company says. The "French Disconnection" is deceptive in appearance. It seems to be a classic antique telephone, tastefully plated in gold toned metal. It looks like a decorator's idea of the perfect touch for an executive's private line. However, the "French Disconnection" in fact contains a new miniaturized device called the Wiretap Trap. With the turn of a knob, the WT system automatically renders any illegal wiretap, present or future, totally inoperable. If the executive prefers to "beat them at their own game" he may decide which calls he will permit a wiretapper to hear and which he will not. By turning the knob further, he can defeat the tap for any given call and cause the wiretapper to hear only static on his tape. A remarkably sophisticated electronic system, the "French Disconnection" is the first product designed to totally control any possibility that an important telephone line is not a private one, according to manufacturer.

For details write Communication Control Corp., 441 Lexington Ave., N.Y., N.Y. 10017, or use reader service coupon, identifying with No. 1707.

Industrial Purchasing Agent
August 1974



PHONE TAPS
NOW MADE
IMPOSSIBLE

Our exclusive equipment detects and defeats illegal wiretaps and room bugs to safeguard the privacy of your home or office. Permanently. Call or write in confidence Ed Green (212) 682-4637

CCC COMMUNICATION CONTROL CORP.
441 Lexington Ave., New York 10017
Dealer Inquiries Invited.

Wall Street Journal
August 6, 1974

Announcing our Spring schedule of **ANTI-WIRETAP & ANTI-BUGGING WORKSHOP SEMINARS**

You are cordially invited to attend a one-day seminar on the latest electronic counter-surveillance equipment and techniques that detect and cancel out "bugs" on your phone lines, equipment and hidden in rooms. The seminars are conducted by highly qualified professionals with over 40 years experience in this field.

Select the date convenient for you and write or phone to register or to request further information.

May 7 May 14 May 22 May 28
June 4 June 11 June 18 June 25

Registration Fee is \$150.00

Contact: Blaine G. Fjellstrom

Communication Control Corp.
441 Lexington Avenue, New York, N.Y. 10017
Telephone: (212) 682-4637

Security Management
May 1975

High Profit Potential

In Booming New ANTI-WIRETAP MARKET

Exclusive equipment locates and permanently cancels out illegal telephone taps and bugs.

NO TECHNICAL KNOWLEDGE NEEDED

Some areas open—
Distributorships available.
Initial investment as
low as \$1500.

Financing available.

Foremost firm in telephone security.

Contact Frank Green

COMMUNICATION CONTROL CORPORATION

441 Lexington Avenue
New York, N.Y. 10017

(212) 682-4637

DON'T LET YOUR CONVERSATION BE BUGGED.

This mini transmitter is of the type found inside a martini olive.

battery

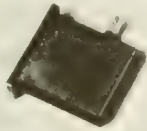
transmitter inside pen

Fountain pen transmitter discovered at a recent "Insiders' Meeting" of Stockholders. The fountain pen actually writes.



"Bug" found in the drop-ceiling of 9 of the 10 bedrooms in a motel leased by a company for its executives during a regional conference. The cleaning man changed the batteries weekly.

Very high frequency and powerful telephone bug planted amid the regular relay equipment. Signal was discovered over 2 miles away from the executive office where it was planted.

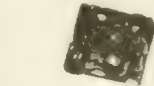


Remote control starter for a tape recorder found in the telephone exchange equipment in the basement of a large chemical company.



Telephone bug with a very low frequency, extremely difficult to detect.

Two of seventeen telephone drop-in transmitters that saturated the executive planning office of a large union. The transmitters fit into the mouth piece of the phone and are identical in appearance to regular equipment.



Amplification stage of a powerful room bug found in the office of a prominent New York law firm.



Low powered telephone tap found in the base of a desk phone of an oil company executive.

This radio transmitter was concealed in the base of a desk pen set used by a Marketing Director of an automobile manufacturer.



These batteries powered a room bug found in the conference room of an advertising agency. Good for approximately 200 hours of transmittal time. The transmitter was confiscated by the authorities.



Parallel type telephone bug found on a telephone pole with self-contained, undetectable battery. This type of device is commonly used by the underworld.

The above devices, all deactivated, are from the collection of Communications Control Corporation

CCC eliminates illegal bugs and wiretaps permanently

Our service includes:

- Electromagnetic and radiation sweeping.
- Telephone and wire security evaluation.
- Physical search.
- Training of your security personnel to preclude future illegal intrusions.
- Complete report of all illegal bugs, together with the areas of potential and actual exposure.
- A check list designed to secure your privacy.

Bugs are found in telephones and rooms belonging to anyone!

- President's office
- Board rooms
- Treasurer's office
- Controller's office

Any key executive offices:

- Marketing
- Research & Development
- Advertising-P.R.
- Design
- Conference rooms

and Other locations

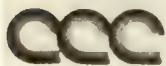
- Corporate apartments, condominiums and hotel suites
- Homes
- Cars, limousines
- Corporate airplanes

The CCC Wiretap defeat system will afford absolute privacy on your telephone lines.



Patented 1960-1961

The CCC "Bug" detector kit is an invaluable aid in the detection of unauthorized transmissions



COMMUNICATION CONTROL CORPORATION

441 Lexington Ave. New York, N.Y. 10017 • Te. (212) 661-3620
creators of exclusive anti-wiretap and anti-bugging equipment and services.

Dealer inquiries welcome

BUG ALERT MODEL EJ3

Patent Pending

This compact, ultra-sensitive instrument gives you an immediate warning when someone wearing a bugging device enters the room. The warning is given by meter and light, either of which can, at your discretion, be turned off so as not to show.

The Bug Alert can be placed in a drawer or behind a picture or in any small, concealed space so as not to be visible to others in your presence.

It detects any hidden transmitter as far away as 20 feet. You can tell at a glance whether your conversation is being "bugged" for transmission to an outside person or recording device.

You can also use it to locate a "bug" previously hidden in a room.

Easily portable, the unit is ideal for use at your office, home, or on your travels . . . wherever you want to be certain of the privacy of your conversations.

- Compact, unobtrusive, easily hidden in a small, secluded space.
- Portable for handy use wherever you want to be sure of your conversation's privacy.
- Also effective as companion equipment with the CCC "BUG" DETECTOR KIT.



DISTRIBUTED BY


COMMUNICATION CONTROL CORPORATION

441 LEXINGTON AVENUE • NEW YORK, N.Y. 10017

212/482-4837 • Cable Address: "ANTITAPS" • Telex 425313



COMMUNICATION CONTROL CORPORATION

April 1st, 1975

Dear Sir:

Members of your Security Department staff are invited to attend:

A SEMINAR: COUNTER-SURVEILLANCE TECHNIQUES AND EQUIPMENT

**Wiretapping and Bugging Techniques and the Countermeasures
Available**

WHEN: Wednesday, May 7th, 1975

WHERE: The Copeley Plaza Hotel, Copeley Square, Boston

TIME: 9.30 a.m. - 5.00 p.m.

As you undoubtedly know, industrial and commercial espionage have reached epidemic proportions in this country.

Still reeling from the effects of Watergate, this nation has learned what those of us in the security field have long known: that wiretapping and illegal bugging are commonplace in every area of American life.

Our organization is one of the leaders in the counter-surveillance field. We have trained and supplied with the most up-to-date equipment security personnel in many of New York's largest corporations, as well as law enforcement agencies and private investigators across the country. We also manufacture the most sophisticated anti-wiretap and anti-bugging equipment on the market today.

Our special seminars in counter-surveillance techniques and equipment have received wide praise from law enforcement officers, as well as security directors of major corporations. Now, we are responding to the many requests we have had to hold a counter-surveillance seminar in the Boston area.

If you would like to have representative of your security staff attend the seminar, please fill out the enclosed registration form and return it to us with your check by Monday, April 28th. Since attendance is limited, I urge you to reply promptly.

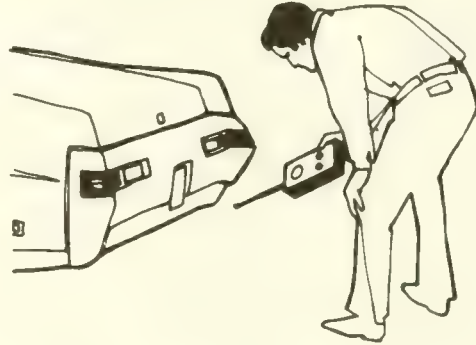
Very truly yours,

Robert Soames
Vice President

441 LEXINGTON AVENUE • NEW YORK, N. Y. 10017 • 212/682-4637 • Cable Address: "ANTITAPS" • TELEX: 425313

BUMPER BEEPER DETECTOR

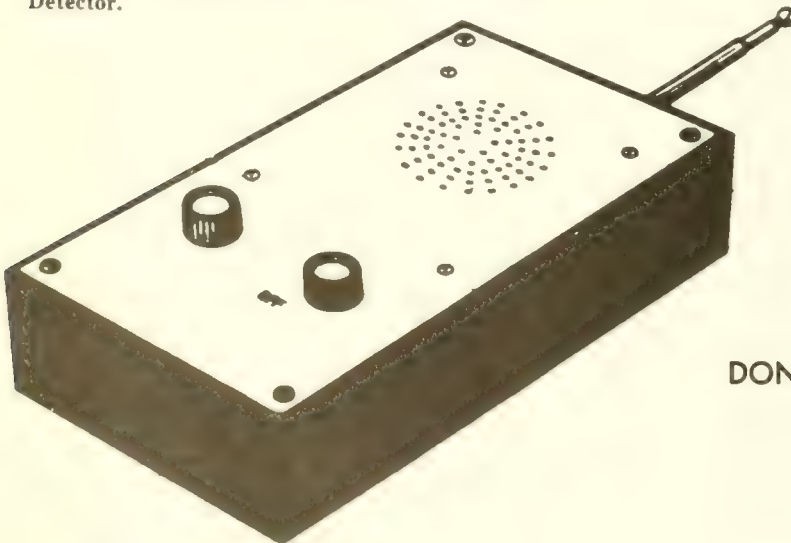
BUG & TRANSMITTER WIRETAP DETECTOR



No unit on the market today can beat
the coverage or ease of operation.

COMPARE THESE FEATURES . . .

- Will detect a bug through one foot solid concrete.
- Bugs hidden in woodwork or walls easily located.
- Tunes itself automatically from 6 kilocycles to 10,000 megacycles, giving widest range of any detector made to date.
- Will cover any room in one sweep where other units must be retuned at each range and the room covered over and over again.
- A room that could take up to 8 hours and 45 minutes to properly cover with other units, can now be done in less than 3 minutes with the new Detector.
- Simple enough for a child to operate.
- All transistor on printed circuit board.
- The enormous range covering ability lets you find bugs planted by professional espionage spies or nosey amateurs.
- Built-in speaker tells you automatically when you are near bug.
- Detects F.M. and A.M. radio waves, radar, closed circuit TV, and F.M. operated cameras.
- Can be used with or without earphones.



\$99⁵⁰

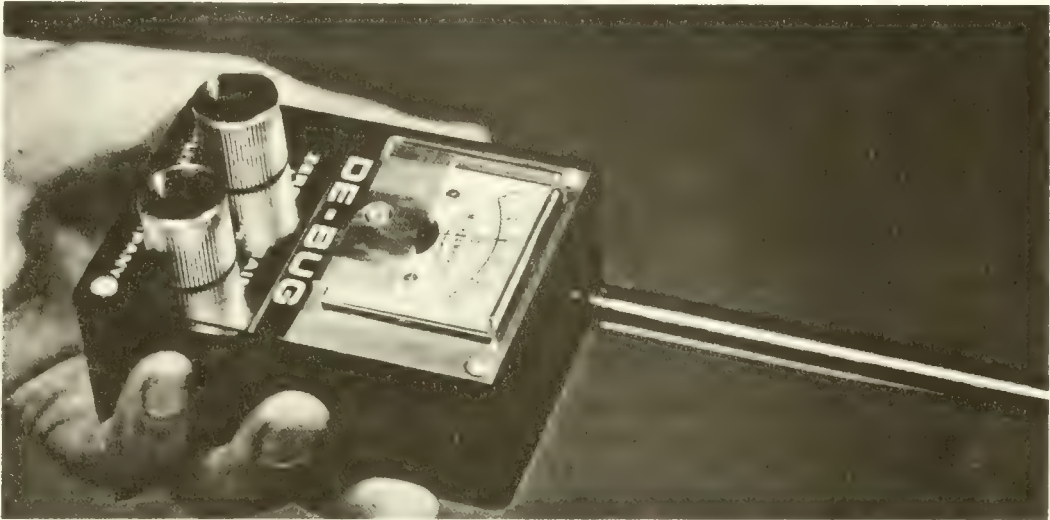
DON-Q & ASSOCIATES

P. O. BOX 548

SEATTLE, WASHINGTON 98111

DE-BUG TRANSMITTER LOCATOR

Do not be victimized by electronic intrusion devices.



Electronic eavesdropping or "bugging" in the United States and throughout most of the world today is big business. Bugs are used by businessmen to steal their competitor's secrets, by private detectives to obtain evidence or information for their clients, and by government at all levels, municipal, state and federal, to invade your privacy for whatever reason they deem necessary (usually unnecessary). Even husbands and wives do it.

These diabolical devices are so easily purchased or built that anyone's conversation may be bugged. Although Federal Communication Commission regulations prohibit the sale or use of these devices, their availability and their very low signal strength make it impossible to enforce these regulations.

The most common type of "bug" is the miniaturized radio transmitter. It may be planted anywhere and its signal picked up at a safe and convenient location. Most transmitter devices are

located by RF field strength measurements. The normal procedure is to scan all frequencies that might be used by a eavesdropper and hope that you are close enough to the "bug" to get a meter reading. This is a haphazard and time consuming exercise which can sometimes take days. The need for a more efficient instrument is obvious.

DE-BUG is such an instrument incorporating the latest state-of-the-art solid state technology. With only two controls, the Model ULD 24 is as simple to use as a transistor radio. A quick "sweep" around a room will determine if you have an intruder.

Broadbanded, no tuning is required and no part of the RF spectrum is missed and so super sensitive it can detect the lowest powered intruder.

We know you will find the DE-BUG an extremely well designed instrument which will prove invaluable to your peace of mind.

HLE

H. L. B. SECURITY ELECTRONICS, LTD.

211 EAST 43RD STREET, NEW YORK, NEW YORK 10017

(212) 986-1367

DE-BUG TRANSMITTER LOCATOR

Do not be victimized by electronic intrusion devices.



Electronic eavesdropping or "bugging" in the United States and throughout most of the world today is big business. Bugs are used by businessmen to steal their competitor's secrets, by private detectives to obtain evidence or information for their clients, and by government at all levels, municipal, state and federal, to invade your privacy for whatever reason they deem necessary (usually unnecessary). Even husbands and wives do it.

These diabolical devices are so easily purchased or built that anyone's conversation may be bugged. Although Federal Communication Commission regulations prohibit the sale or use of these devices, their availability and their very low signal strength make it impossible to enforce these regulations.

The most common type of "bug" is the miniaturized radio transmitter. It may be planted anywhere and its signal picked up at a safe and convenient location. Most transmitter devices are located by RF field strength measurements. The normal procedure is to scan all frequencies that might be used by a eavesdropper and hope that you are close enough to the "bug" to get a meter reading. This is a haphazard and time consuming exercise which can sometimes take days. The need for a more efficient instrument is obvious.

DE-BUG is such an instrument incorporating the latest state-of-the-art solid state technology. With only three controls, the Model ULD -370 is as simple to use as a transistor radio. A quick "sweep" around a room will determine if you have an intruder.

Broadbanded, no tuning is required and no part of the RF spectrum is missed and so super sensitive it can detect the lowest powered intruder. The acoustic verifier feature provides positive feedback identification of an intruder. You are not misled by other RF sources such as nearby broadcasting stations, noisy neon starter switches, and etc.. In feedback verification the intrusion device hears itself amplified thus forming a closed loop, the cycle repeats until there is a continuous whistle or scream. This can only happen obviously if there is a transmitter present.

Other features include separate antenna probe for those hard to reach spots, headphone jack, recorder jack, and collapsible handle for easy stowage.

We know you will find the DE-BUG an extremely well designed instrument which will prove invaluable to your peace of mind.

HLB

H. L. B. SECURITY ELECTRONICS, LTD.

211 EAST 43RD STREET, NEW YORK, NEW YORK 10017

(212) 986-1367

TELEGUARD 1000 ————— LINE TAP DEFEAT SYSTEM

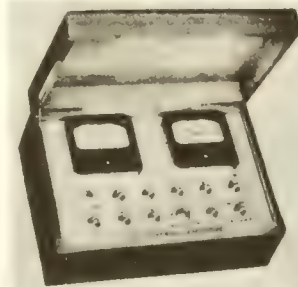
The TELEGUARD 1000 , a major electronic breakthrough, will
 afford absolute privacy on your telephone lines in a unique system never available before. It
 will render ineffective sereptitious electronic wire taps that may be on your line right now, ..
or can be added at any time.

The TELEGUARD is the successor to a complete line of sophisticated equipment designed
 solely to DETECT and DEFEAT ILLEGAL ELECTRONIC WIRE TAPS. Operating on a
 BALANCED LOOP PRINCIPLE, similar to a Wheatstone Bridge, the TELEGUARD will
 perform the following:

- ANALYZE, BALANCE and SECURE *your telephone lines.*
- DEFEAT PARALLET WIRE TAPS.
- DEFEAT ELECTRONIC TELEPHONE STARTERS.
- DETECT and DEFEAT SERIES WIRE TAPS.
- DETECT and DEFEAT INFINITY TRANSMITTERS.
- DETECT UNAUTHORIZED TELEPHONE EXTENSIONS IN USE.
- *Operates on incoming as well as outgoing calls and can be used on both sides of the line, in pairs.*
- PORTABLE. *Can be used on any phone.*
- NO BATTERIES or A.C. *supply needed.*
- SIMPLE INSTALLATION. *Plug the TELEGUARD into your wall jack, plug your telephone into the TELEGUARD jack.*

TELEGUARD 1000 ➡

- *All solid state circuitry. Will last indefinitely.*
- *Analyzes, Balances and Secures your telephone lines.*
- *Solid Walnut Case. 9x6x2.*
- *Two year guarantee.*
(Free replacement if defective.)



HLB

H. L. B. SECURITY ELECTRONICS, LTD.

211 EAST 43RD STREET, NEW YORK, NEW YORK 10017
 (212) 986-1367

THE PHONE SWEEP

STONE SWEEP ANY PHONE LINE IN THE U.S.A. RIGHT FROM YOUR OWN OFFICE

WHY STONE SWEEP A PHONE LINE?

Because today, it is common knowledge that thousands of tone activated eavesdropping microphones have been sold and installed on phone lines throughout the U.S.A.

WHAT IS A STONE ACTIVATED PHONE LINE MICROPHONE?

These microphones are so common that they have even been advertised in national mail order catalogues. They may be installed on the line anywhere inside the premises and will send all room voices back over the phone line to the user. They can now be turned on from any other phone in the U.S.A. by direct dialing. The user simply dials your number and sends a tone signal over the line simultaneously. Your phone does not ring while this is happening. And yet he has taken over your line from wherever he may be, and can now listen to your most private conversations as long as he desires. The mike is turned off only when he decides to hang up.

HOW THE PHONE SWEEP FINDS THE MICROPHONES

All of these microphones, from the oldest to the newest, have one thing in common. They must be activated (turned on) by a tone signal on the line. The tone may be any chosen frequency between 300 and 2000 cycles. The PHONE SWEEP generates a tone signal which sweeps through all of these frequencies. After you dial the number that you wish to check, place the PHONE SWEEP to the mouthpiece of your phone and turn on the switch. It takes only one minute for a complete sweep. This method is accurate and will never miss. To check your own phone, dial your number from any other phone you choose. You may even use a coin phone if you wish. You will hear the tone and will know when the sweep is completed. Turn off the PHONE SWEEP and listen for the ring signal to the other phone. If it is still ringing, there is no tone activated mike on it. If it is not ringing, and no one has picked up the other phone, then you have turned on a tone activated microphone on that line. If any sounds are present at the premises, you will now be able to hear these sounds.

FINALLY

It takes no great amount of imagination to contemplate the profits available to you, by sweeping the lines of your clients on a regular basis. Do it right from your own office. Any phone in the U.S.A. that you can dial direct. Takes only one minute after you have finished dialing. Naturally some of your clients will insist on buying the PHONE SWEEP and you may optionally sell them at whatever price you deem adequate.



ALUMINUM CASE
1.3 x 2.9 x 8.3 INCHES



NO WIRES TO CONNECT
ONE YEAR WARRANTY

AVAILABLE FROM:

R. B. CLIFTON
11500 N. W. 7th AVE.
MIAMI, FLORIDA 33168
PHONE 305 - 681-1813

ONLY \$138⁰⁰

Shop by Mail

Eavesdropper Stopper



How private is your phone? The U.S. Census Bureau and the Federal Bureau of Investigation are warning that you may be giving away more information than you realize. With a few simple steps, you can help protect your privacy. Be sure to use a secure phone line when you call the Social Security Administration, the Internal Revenue Service, or your bank or utility company. Don't give out your name or telephone number to strangers, and don't give out your name or address to anyone who calls you. If you're a resident of a long-term care facility, make sure you're protected from unauthorized access to your information.

Order No. 43710: Eversdropper Blipper \$79.95
plus \$2 pstg & hndg.

The Gallery, Dept. 3904, Amsterdam, N.Y. 12010

TOLL FREE CALL FOR CREDIT CARD

HOLDERS 800-833-6231

IN NEW YORK CALL (518) 842-6000.

The **GALLERY**
OF AMSTERDAM

CHAIRMAN ERICKSON: We will proceed with the next panel.

We welcome these members to the Commission:

Mr. Milo A. Speriglio, Chairman of the Board and Director and Chief of four private investigation firms.

Mr. Philip Nesbitt, Assistant Director of Investigations, and head of the Electronic Countermeasures Division of Pinkerton's.

Mr. Samuel W. Daskam, President of Mason Technical Security Services, and General Manager of F. G. Mason Engineering, Inc.

All these men have had many years of experience in providing electronic countermeasures surveillance, and we again thank you for appearing.

Will you gentlemen step forward and be sworn?

[Whereupon, Messrs. Speriglio, Nesbitt and Daskam were sworn by Chairman Erickson.]

**TESTIMONY OF PANEL ON
COUNTERMEASURE SERVICES:
SAMUEL W. DASKAM, GENERAL
MANAGER, F. G. MASON
ENGINEERING, INC.; MILO A.
SPERIGLIO, DIRECTOR & CHIEF,
NICK HARRIS DETECTIVES, INC.;
H. PHILIP NESBITT, ASSISTANT
DIRECTOR OF INVESTIGATIONS,
PINKERTON'S, INC.**

CHAIRMAN ERICKSON: Mr. Hershman.

MR. HERSHMAN: Gentlemen, if you have opening statements, I'd appreciate it if you'd limit them to five minutes.

Mr. Speriglio, would you like to begin?

MR. SPERIGLIO: General Hodson, Chairman Erickson and distinguished members of the National Wiretap Commission, it is an honor and a privilege to accept this invitation to testify before you.

I am Milo A. Speriglio, Chairman of the Board and Director and Chief of four private investigation firms based in Los Angeles, California. Nick Harris Detectives, Inc., the parent corporation, was founded in 1906 and now includes California Attorneys Investigators, Inc., Milo and Associates, and Scientific Investigation Agency.

As we know, the 90th Congress enacted Public Law 90-351 cited as the Safe Streets Act of 1968. It prohibits unlawful interception of private communications through bugging and wiretapping and provides for criminal penalties and civil damages against its violators. The Act makes it illegal to manufacture, distribute, or possess electronic eavesdropping devices. Many experts agree the Act did not drastically alter the pattern of electronic

espionage. Your task, as I see it, is, in part, to determine the effectiveness of that Act. In my professional opinion, the so-called electronic invasion is nearing an epidemic stage in the United States.

Recently, I completed a manuscript for a book entitled, *SHHH!* It illustrates how commonplace bugging actually is in today's society. Our Los Angeles office repeatedly refuses to accept bugging assignments. One of the book's chapters is, "We Turn Down a Million Dollars a Year," a conservative estimate. Many of the individuals, associates and corporations who request eavesdropping installations actually believe it is legal and know nothing of the Act of 1968. Eventually, they will find someone who will do their bugging for them, or will ultimately do it themselves.

It's easy for anyone to obtain bugging devices. While I was preparing this statement, my secretary handed me a letter mailed from St. Louis. The letter is typical of the hundreds of such unsolicited advertisements selling bugging devices which we have received since 1968. This letter included an advertisement featuring a device that would automatically record incoming and outgoing telephone calls. The retail price was \$29.95, or in quantities of ten or more units, it dropped to \$23.37.

As with all such advertisements after 1968, it contained a disclaimer. This one stated, "Note: Some states may prohibit recording conversations without both parties' advance agreement." It so happens that one of those states is California. Telephone conversations can be recorded in California if a beep tone is given. They clearly pointed out in their advertisement, however, that their Model 4 does not emit a beep.

While the cost of almost everything we purchase today has increased, bugging devices are costing less than ever before. Many of us have pocket calculators. They are now available for only a fraction of what they sold for before they were mass-produced. Today anyone can afford to purchase a bug.

Aside from my opening statement, I just want to bring to the Commission's attention, as I flew out here on the airplane I was reading the most current issue of *Playboy* magazine. It contained on page 194 an advertisement reading in part, "Miniature transistors. Picks up and transmits most sounds without wires through FM radio up to 300 feet. Use it as a mike. Use it as a babysitter, burglar alarm, hot line, et cetera, for fun, home, or business. Cost, \$14.85."

Back to my opening statement.

Potential targets of privacy invaders often become victims of "black box operators" as my

colleagues call them. Unscrupulous instant-experts claim they can locate and remove hidden wiretaps and bugs. The man with the black box has no credentials, is not a state licensed investigator, and pretends to be an electronic debugging expert. He preys upon the countless thousands of individuals and firms who suspect they are under electronic surveillance. His countermeasure equipment is ineffective, yet impressive looking, displaying flashing lights, meters, or emitting sounds. Many of the black box operators build their own debugging equipment from a few dollars worth of components. Since Watergate, countermeasure equipment has been mass-produced throughout the nation. Some units sell for more than \$1,000 and contain less than \$45 worth of parts and labor.

Another chapter in my manuscript is titled, "Find Help Fast in the Yellow Pages—Like Hell." Approximately 85 per cent of the nation's telephone subscribers are customers of the Bell System or General Telephone. If they suspect their phone is tapped or their room is bugged, they cannot find professional help in the yellow pages.

In 1972, the Bell System decided to ban the advertising of debugging services in the yellow pages. This censorship included everyone, even those who are licensed by the State to perform this much needed service.

Pacific Telephone Company is Bell's second largest system. Their tariff, filed with the Public Utilities Commission, is similar in language to others filed. It states:

"(We) prohibit the acceptance of advertising either stating or implying:

"Detection of eavesdropping devices

"Privacy secured by detection of electronic equipment

"Hidden microphones detected

"Electronic bugs uncovered

"Debugging and

"Bug-finding service"

As a direct result of the phone company's position, I conservatively estimate that thousands of wiretaps and room bugs have gone undetected.

In April of this year, one of my firms submitted an advertisement for the Los Angeles Central Yellow Pages. One line of copy referred to me as the author of the manuscript I previously mentioned. It stated, "*SHHH!*, a book about phone tap detection." It was rejected, as they would not allow such description in the yellow pages.

An alternate description was submitted. It read, "A book about privacy invasion detection." It, too, was banned.

Next, we submitted the words, "A book about your right to privacy." Once more, top-level management rejected it.

As a last resort, we changed the copy to read, "A book about your constitutional right to privacy." Their immediate reply was, "You cannot use the words 'right to privacy' in the phone book." I then reminded them of the Fourth Amendment to our Constitution. They finally agreed to permit this statement describing the book.

The phone company takes this arbitrary position to censor advertisements from legitimate companies that are qualified to detect illegal wiretaps and room bugs. We must ask ourselves, "Why?"

Thank you for giving me the opportunity to shed some light on this monstrous problem which faces our entire nation. I now stand ready to answer your inquiries, but first may I introduce some documents to be entered into the record.

CHAIRMAN ERICKSON: Of course, we will welcome the documents. The documents that you are offering—have you previously provided those to Mr. Hershman?

MR. SPERIGLIO: No, I haven't.

CHAIRMAN ERICKSON: Would you come forward and hand them to Mr. Hershman?

MR. SPERIGLIO: Would you like a brief description of any of them?

CHAIRMAN ERICKSON: Yes.

MR. SPERIGLIO: I will give you a copy of the *Playboy* advertisement.

I will give you a copy of the public utilities tariff for the Pacific Telephone part of the Bell System.

I will give you a copy of the General Telephone Company's tariff filed with the Public Utilities Commission.

I will provide you with a letter from the Public Utilities Commission, State of California, which states that according to the phone company they are acting in this manner, prohibiting advertisement of debugging as a result of the Safe Streets Act of 1968. The phone company takes the position that they are doing this as a result of that act which, as we all know, only prohibits wiretapping, not detecting it.

I will also provide you with a copy of the recent advertisement I received that I mentioned in my opening statement, a copy of an advertisement submitted to Pacific Telephone Company, which was rejected.

And one letter I'd like to read you in part to show how widespread bugging actually is. It says:

"Occasionally bugs do break down. We all know these things can happen. That is what we are here for. Interelectronics is a new firm, but we know our business and we are prepared to provide all types of surveillance equipment. In this day of complex gadgetry and highly sophisticated techniques, it is par for the course to have a mechanical failure now

and then. That is what we are here for. We are not expensive. We do things fast and clean. We hope you will call upon us. We are here to help."

This just points out that there are a lot of bugs on the market if there are companies to repair them.

I will submit them to you.

MR. HERSHMAN: Thank you.
[The material referred to follows.]



MINIATURE TRANSMITTER
WIRELESS MICROPHONE

Among world's smallest improved solid state design. Picks up and transmits most sounds without wires thru FM radio up to 300 ft. Use as miko, music amp, baby sitter, burglar alarm, hot line, etc. For fun, home and business. Batt. incl. Money back guar. B/A. M/C cds., COD ok. **Only \$14.95** plus 50¢ Post and hdg. **AMC SALES, Dept. P, Box 928, Downey, Ca. 90241.**

Size
1 1/4 x 3 4 x 1 1/2

STANDARDS FOR YELLOW PAGES ADVERTISING CONTENT

(INSTITUTIONAL COPY, CONT'D)

- The listings of the members in the listing columns are identified by extra lines of information such as, "Member of _____ Association," etc., or are identified under a Trade Mark Heading, Trade Name, or in the case of reference to display advertisements, the advertisements are especially identified by emblems, statements or other significant identification.
- Particular attention is given to the copy to make it clear to the directory user that any endorsement is made by the association or group involved, and not by the Telephone Company and to make certain that there is no implication that only those listed as members of a group are qualified to perform the particular services involved and that those not listed as members are not qualified.

INSULATION CONTRACTORS — See "Contractors"

I-INSURED

The word "Insured" shall not be advertised unless qualified by the inclusion of the type of coverage.

FOR EXAMPLE:

- "We carry full liability insurance."
- "Your property is fully insured while in our possession."
- "Insurance coverage may be arranged."
- "Insurance Available."

I-INTEREXCHANGE RECEIVING SERVICE LISTINGS (IRS)

Directory listings are provided in accordance with schedule 17-T.

The telephone number prefixes are:

- "Enterprise" in Northern California and Nevada
- "Zenith" in Southern California

At the option of the subscriber, the listing may be non-published.

The phrase, "No inter-city charge" may be included if the subscriber so desires.

Advertising copy containing (IRS) numbers, must include the names of the (IRS) sending exchanges located in the classified directory area and "Ask operator for" or "Ask long distance for" instructions.

INVESTIGATORS

It may be unlawful for firms or individuals who are not State licensed as Private Investigators to be represented under this heading. Furthermore, in California, it may be unlawful for one who is licensed not to use the name and address as they appear in State records.

See "Address is Required"

- II- In California, copy which infers that the advertiser offers to procure or obtain, or to aid in procuring or obtaining, any divorce, severance dissolution or annulment of any marriage may violate section 159a of the California Penal Code

I- We have long prohibited the acceptance of advertising either stating or implying that wire tapping or eavesdropping is employed by the advertiser. This standard not only prohibits the advertising of wire tapping and eavesdropping devices, but also so-called debugging advertising (i.e. advertising stating or implying electronic devices or services will be provided for the detection and removal of wire taps and eavesdropping "bugs") on the basis that those who can debug also possess the capability to bug and wiretap

(continued)

STANDARDS FOR YELLOW PAGES ADVERTISING CONTENT

(INVESTIGATORS, CONT'D)

Following are examples of the type of phrases that are prohibited from appearing under any heading in the Yellow Pages:

UNACCEPTABLE

- Electronic Surveillance
- Secret Records
- Eavesdropping
- Wiretapping
- "Bugging" or "De-bugging"
- Secret Listening Devices
- Bug Finding Service
- Detection of Eavesdropping Devices
- Privacy Secured by Detection with Electronic Equipment
- Hidden Microphones Detected
- Listening Devices
- Electronic Bugs Uncovered

ADVERTISING UNDER THE HEADING INVESTIGATORS

I- Phrases such as "Electronic Equipment," "Electrical Devices," etc., without further qualification may imply that wiretapping, bugging or debugging equipment is being employed. These ambiguous phrases cannot be permitted to stand alone under the heading Investigators. These phrases may be mentioned in copy only if qualified with additional, specific descriptive information which clearly discloses that the device or equipment is to be used for a purpose other than wiretapping, bugging or debugging.

Following are examples of the type of unacceptable and acceptable phrases under the heading Investigators.

UNACCEPTABLE

- Electronic Devices
- Electronic Equipment
- Electronic Protection Equipment
- Electronic Security
- Surveillance Equipment
- Security Equipment
- Specialized Electronic Equipment
- Electro Magnetic Devices
- Electronic Sensing Equipment

ACCEPTABLE

- Electronic Security Equipment for the prevention of shoplifting
- Specialized Electronic Equipment for the detection of burglaries
- Electronic Sensing Equipment for the detection of fire

There are a few instances under Investigators where the mention of specific equipment, even though qualified, may still imply that wiretapping, eavesdropping or debugging services are being provided by the advertiser. This would include, for example, mention of such devices as tape recorders. While a tape recorder may be a component of an acceptable service, its role is normally so minor or obvious as not to warrant its being highlighted in the advertisement. Accordingly, in such instances calling attention to such recording equipment serves no useful purpose and can only be interpreted as a subterfuge designed to circumvent the intent of these standards.

ADVERTISING UNDER THE HEADINGS FOR SECURITY PRODUCTS AND SERVICES

I- There are a number of specific headings (see list below) which require close scrutiny for possible violation of the intent of these standards. Normally, it would not be necessary to qualify phrases such as "Electronic Devices" under the headings (listed below) since the heading itself (e.g., Burglar Alarm Systems) provides the necessary specific descriptive information. However, if there is an implication in an advertisement that wiretapping, eavesdropping or debugging services are employed, the advertisement must be modified to conform to these standards.

- Burglar Alarm Systems
- Fire Alarm Systems
- Guard Dogs
- Home Protection Equipment & Supplies
- Iron Safes
- Life Detection Service
- Police Equipment
- Security Control Equipment & Systems
- Security Systems Consultants
- Shielding Protection Device

(continued)

STANDARDS FOR YELLOW PAGES ADVERTISING CONTENT

(INVESTIGATORS, CONT'D)

THE EFFECT OF ADVERTISEMENTS TAKEN AS A WHOLE

I—Finally, some advertisements as a whole may be completely unacceptable although every phrase, separately considered, may meet the requirements of these standards. Thus may be "because things are omitted that should be said, or because advertisements are purposely composed or printed in such ways (e.g., through illustrations, graphic arrangements, or size of type) as to lead the reader into believing that wiretapping, eavesdropping or debugging services are available. As publishers of the Yellow Pages, the Telephone Company must exercise sound judgment and reject such advertisements whenever an advertisement as a whole conveys the impression that wiretapping, eavesdropping or debugging may be employed.

JAIL EQUIP — See "Wire Tapping"

STANDARDS FOR YELLOW PAGES ADVERTISING CONTENT

IDENTIFICATION EQUIP & SUPPLS — See "Wire Tapping"

I—ILLEGAL BUSINESS

Advertisements of businesses or activities which are illegal, for example, book makers (bookies), gambling parlors or gambling devices, etc., are unacceptable.

I—ILLUSTRATIONS

Copyrighted illustrations, illustrations which have appeared in another advertiser's announcement, or trademark names or symbols not the property of the advertiser will not be accepted unless the advertiser has secured proper permission.

Portraits or pictures of people are not acceptable for half tone or line etching reproduction unless the people in the picture give written authority to the Telephone Company.

An illustration of a building which attempts to convey the idea that the advertiser occupies the entire premises is not acceptable unless such is the case.

See also "Objectionable Copy" — "Brand Name Control Section"

INDUCEMENTS — FINANCIAL — See "Financial Inducements"

I—INFORMATIONAL LISTING COPY

An Informational Listing is a listing that has been split to permit the inclusion of informational copy between the listed name and the address and telephone number. At least one line of informational copy must be provided with this listing.

The firm name must always agree with the name in the customer's alphabetical listing. It is not permissible, under any circumstances, to edit or abbreviate the firm name in an informational listing which would result in a difference between the alphabetical and classified listings.

Address and telephone numbers of branches, etc., may be shown under the Informational Listing address and telephone number provided the branch alphabetical listings are in the exact same name as the Informational Listing.

Directional lines of information such as "Across from Palace Hotel," "Between Polk and Larkin," etc., should normally appear in copy above the address. However, if requested by the advertiser, this information may appear below the first address.

Lines of reference information, such as "If no Answer Call _____" and "Between _____ PM & _____ AM" or a "Residence" indent, may also appear below either the main or branch locations. A "Residence" indent, however, may only be shown if the business listing clearly identifies the name of the subscriber to, or an additional listing on, the residence service.

Names and addresses (but not telephone numbers) of firms represented by the advertiser are acceptable in copy when preceded by such words as "Representing," "Agency for," etc.

See also "Misleading Advertising Copy" — "Unacceptable Advertisements"

I—INSTITUTIONAL COPY

Where the advertiser is a professional or trade association or a similar group generally recognized and accepted as such in the profession or trade, the advertisement shall not identify the members. It may, however, include a reference to the listings of the members in the listing columns of the directory or to their display advertisements, provided that

1. The advertising copy is of an institutional nature limited to publicizing the association, its purposes or policies, its significance, qualification for membership, etc., and the reference to the listings or display advertisements of the members serves only to identify them as such.

(continued)

WARRANTY - See "Guarantee"

WATERPROOFING CONTRACTORS - See "Contractors"

WEATHER STRIPPING CONTRACTORS - See "Contractors"

WHOLESALE

The use of the word "Wholesale" is permitted only when the advertiser is in fact in the wholesale business and is so recognized by the trade of which he is part.

See also "Bait Advertising Copy" and "Misleading Advertising Copy"

WIRETAPPING

"Since wiretapping is prohibited by Federal and State Laws, advertising copy for Detective Agencies, Investigative Services, etc., can neither state nor imply that wiretapping is employed. Equally unacceptable is the offering of electronic devices or of services involving the use of such devices for the purpose of wiretapping or eavesdropping. Similarly, advertising copy stating or implying that services will be provided for the detection and removal of wiretapping and eavesdropping apparatus, (i.e., "debugging") is unacceptable.

WRECKING CONTRACTORS - See "Contractors"



Public Utilities Commission

STATE OF CALIFORNIA

June 5, 1972

FILE No. IC 55555-T
Re: Nick Harris
Detective Inc.

California Attorney's Investigators, Inc.
550 South Vermont Avenue
Los Angeles, California 90020

Attention: Mr. Milo A. Spergilio

Dear Mr. Spergilio:

This is in further response to your letter concerning advertising for your client of the above name in telephone directories provided by the Pacific Telephone Company.

As in the telephone conversation with you and our staff member, Mr. Toczauer, he explained that in an attempt to assist you, we requested that the telephone company review your complaint and explain its policy. In response to our inquiry we received the following answer from the telephone company:

"In December 1971 our Company revised its standards for Yellow Pages advertising content pertaining to the Classified Headings of 'Detective Agencies' and 'Investigators' specifically, and all Classified Headings in general. This was done in an effort to comply with the intent of the Federal Omnibus Crime and Safe Streets Act of June 1968. This standard not only prohibits the advertising of wire tapping and eavesdropping devices, but also so called debugging advertising on the basis that those who can debug also possess the capability to bug and wiretap."

Our staff requested that the telephone company once more review its policy and indicate if it is willing to consider any compromise. The telephone company response was that they feel they are obliged to stand firm on these responses.

While our Commission and its staff doesn't necessarily agree with the telephone company interpretation, informally it is in no position to order or instruct Pacific Telephone Company to

June 5, 1972

-2-

alter, modify or change its announced policy.


As it was further explained in the phone conversation between you and our staff member, if you are dissatisfied with the above response you may file a formal complaint with our Commission. Once such a formal complaint is filed, if accepted, hearings are set and in the course of the hearing sworn testimony and other evidence is received. Based on such evidence the Commission will then be in a position to dispose of the above controversy by order. Such orders may affirm the company's present policy or may order it changed or modified as the evidence obtained in the course of the hearings would warrant.

As promised by our staff member, to assist you in appraising the involvements in the formal complaint we are enclosing with our letter a copy of the Rules of Procedure.

Very truly yours,

PUBLIC UTILITIES COMMISSION

WILLIAM R. JOHNSON, Secretary

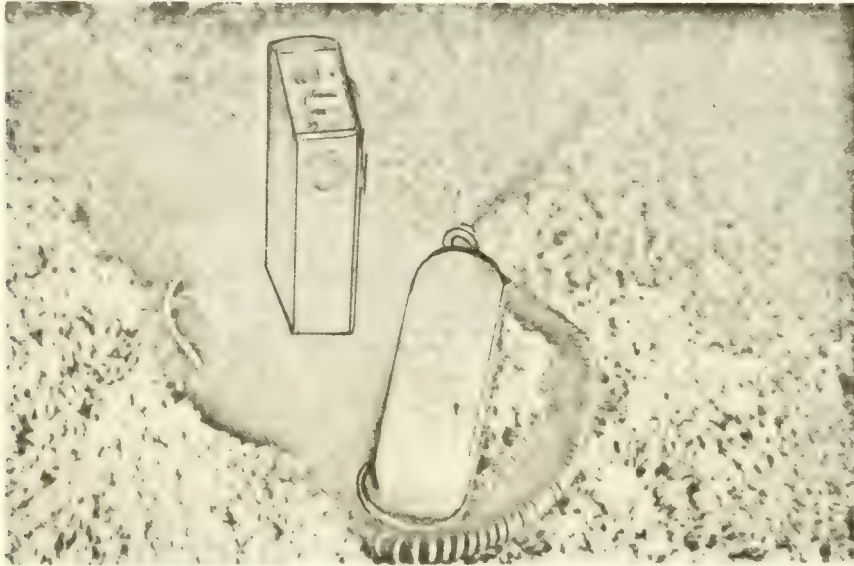
By 
Michael L. McGinley
Assistant Secretary

Enclosure: Rules of Procedure

AUTOMATIC INTERCONNECT DEVICE
(AID)

BRIEF DESCRIPTION

AID is a specially designed coupler that allows remote activation of any tape recorder--directly--any point on the telephone line. Lifting any telephone receiver on that line will activate the tape recorder. This allows a tape recorder to automatically record all incoming and outgoing calls...without unnecessary drain on batteries and tape waste. The unit is completely silent and does not change the clarity or volume of the conversation.



SPECIFICATIONS

Additional equipment.....	Battery or AC operated tape recorder with remote plug.
Additional power.....	None
Technical background.....	No electronic experience necessary
Dimensions.....	1½" x 1" x 1"
Current price.....	24.95
Note.....	Some states may prohibit recording of conversations without both parties advance agreement. AID does not emit an audio beep.

AID is a product of: Metro-Tech Electronics
3338 Olive St.
St. Louis, Mo. 63103
314-533-9970

NEW
STANDARD
DATE

50% from Day

ADVERTISER)

KEEP CLEAR
FOR
DISPLAY
PRODUCTION

Space For Printer

Space For Printer
 DR WITH COPY
 4-16-75
 [Signature]

DARK AS POSSIBLE

YOUR CONSTITUTIONAL
RIGHT TO PRIVACY

10% BEN
DAY

Center two
lines

Miles and associates

**A LEGEND
IN HIS OWN TIME:**
"THE ROYAL" A MOTION
PICTURE ASSOCIATES
WIS ASSOCIATES
AUTHOR OF "SHHHH" ABOUT

**CIVIL - MARITAL
EXPERTS
FOR ROUTINE
OR
DIFFICULT
ASSIGNMENTS
ANYWHERE**

**CIVIL - MARITAL
INVESTIGATIONS
CALL FOR OUR FEES**

386-3800

8:30 AM - 11 PM - 7 DAYS
WILSHIRE CENTER - SUITE 900
550 S. VERMONT AVE. - L.A.

A DIVISION OF
SCIENTIFIC INVESTIGATION AGENCY

NATIONALLY FAMOUS INVESTIGATOR

"A MASTER
DETECTIVE"

N.Y.
N.Y.
N.Y.

"SHADOWING"

FOR PEACE
OF MIND

"PHONE
LOCATED"

WASH. D.C.
WASH. D.C.

BUSINESS
LOSSES

"DETECT-ED"

PRE. 1975

THIS SPACE FOR ATTACHEMENTS ONLY
DISPLAY SECTION

INTELECTRONICS

To All Detectives:

Occasionally bugs do break down!

We all know how these little things can happen.

That's what we're here for.

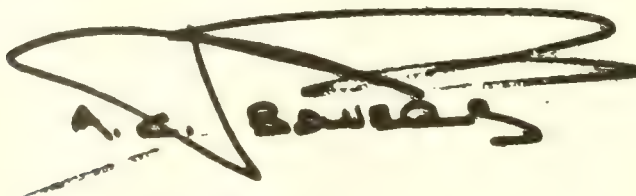
INTELECTRONICS is a new firm, but we know our business, and we are prepared to repair all types of surveillance equipment.

In this day of complex gadgetry and highly sophisticated techniques, it is par for the course to have a mechanical failure now and then. That is what we're here for.

We are not expensive, we do things fast and clean, and we hope you will call us.

We're here to help.

Respectfully,

A handwritten signature in dark ink, appearing to read "A.C. Bowers". The signature is stylized with a large, sweeping loop at the end.

A.C. Bowers
Field Consultant

ACB/sm

P.O. BOX 1874, SANTA MONICA, CA. 90406 • (213) 848-7413

MR. HERSHMAN: Mr. Nesbitt, do you have an opening statement?

MR. NESBITT: Yes, I do, Mr. Hershman.

I am H. Philip Nesbitt of Bethesda, Maryland. At present I am Assistant Director of Investigation and also head the Electronic Countermeasures Division of the Investigative Directorate of Pinkerton's, Inc.

As for my personal qualifications, I am a senior member of the Institute of Electrical and Electronic Engineers and possessor of patents in this field. I have been actively engaged in the electronic countermeasures field for approximately 30 years. During that time I have operated my own company. A little over a year ago I joined Pinkerton's, Inc.

My experience includes the design and fabrication of electronic countermeasures and specialized equipment which has the function of providing greater industrial security and more effectiveness in countering new sophisticated devices.

When I was invited to appear before this committee, I was delighted to accept primarily for two reasons: One, it says to me that there is an awareness that there is a problem in the field of electronic surveillance. Two, my appearance here provides a forum to show you gentlemen, as legislators, just how large and serious this problem is.

Let me hasten to say that, due to the nature of the work that I and my division perform, I am not at liberty to give this committee the specific names of clients for whom this work has been performed. Aside from the fact that their actual identities are irrelevant to what is being investigated here, it would be a violation of our business ethics to divulge the names of our clients.

As to the nature of the problem and its magnitude, let me cite some examples:

In the past we were called upon to check a facility, a legal firm, where we discovered a total of ten taps on eight lines in use—or two lines had been tapped twice.

You are all aware of the "Great Seal" bug found in one of our embassies. This technique has become quite prevalent in recent years. A more sophisticated version of this was mentioned in the press just a few weeks ago.

We've discovered devices in such innocuous things as award-type wall plaques, children's toys and clothes trees, to mention a few.

There has never been lack of interest in the training seminars I conduct, wherein members of the commercial, industrial community and government agencies, including police personnel, are apprised of and instructed in the identification of devices and methods to combat this very serious problem.

As to the effectiveness of Sections 2511 and 2512, my first comment is that, based on my ex-

perience, it is my personal opinion that 2512 as written has an inherent defect. I say that because the devices on the market today which are perfectly capable of illegal electronic surveillance, are being sold as baby-sitting devices, entertainment devices, intercoms, burglar alarms, elocution aids, et cetera. I don't feel it is possible to legislate against the manufacture of such items, but I do feel that there must be some restrictions.

Secondly, under 2512, as now written, I often have the feeling when I go on an investigation that I am breaking the law, which is certainly not my intention. I do possess and carry in interstate commerce, in my work, in the language of the statute, "electronic devices . . . knowing that the design of these devices render (them) primarily useful for the purpose of surreptitious interception of wire or oral communications." I cannot bring myself or my company within any of the exceptions in the statute. Therefore, I would highly recommend that there be incorporated in Section 2512 language which would cover people like myself.

As to Section 2511, I don't feel I'm particularly qualified to comment on that section because the violations outlined there are criminal in nature and seem to me to be the province of the prosecutor rather than an electronics specialist such as I.

I think it might be of interest to the committee to know of two areas where problems exist in this field now and in the immediate future.

One is the pseudo-expert that has surfaced recently. I'm alluding to the self-styled countermeasures technician who, after purchasing a \$29.95 diode detector, and using his limited, if any, training, passes himself off as a true expert in this field and charges in the neighborhood of \$600 to check out one room. This type of person is doing great harm to the people hiring him as he gives a false feeling of security while fattening his wallet. As an indicator substantiating my statement, equipment to do only a passing job costs in the vicinity of \$20,000. I feel there should be some basic national standards set forth to control this problem.

The second is theft of information contained in computers. In spite of protestations to the contrary by many suppliers and operators, computer theft is a very real problem. There are many ways this theft can be accomplished, and with the great upsurge of computer usage, the general public must be made aware of the problems and the limited manner in which they can protect themselves.

But I am not here to talk. Rather, I am here to answer any questions you may have and to be as helpful as I can in this rather esoteric field.

One thing further I would like to say before you begin your questions. Few people in these United

States know of the possibility—indeed, the probability—of electronic espionage, and many of those that do refuse to believe it is indulged in except in isolated cases. Nothing could be further from the truth.

To illustrate my point, I would willingly bet that, given the authorization, I could find bugs right here on Capitol Hill, perhaps even in some of your offices. Even if there are no bugs as such, I know of ways to intercept every phone call you make. I suspect you might want to question me about those “ways.” If so, I would like to request it be done in executive session so that these methods do not become common knowledge.

Gentlemen, I'm at your disposal.

MR. HERSHMAN: Thank you, Mr. Nesbitt.

Mr. Daskam, do you have an opening statement.

MR. DASKAM: I don't have a formal statement. I'd like to make an explanation of the two companies I am involved with.

MR. HERSHMAN: Please do.

MR. DASKAM: Mason Technical Security Services was formed approximately four years ago and really set up for cost accounting purposes since both F. G. Mason Engineering, Inc. and Mason Technical Security Services, Inc. are owned by Francis Mason.

The F. G. Mason Engineering Company was formed in 1960 strictly as a manufacturing and engineering firm for countermeasures equipment for the United States Government. Approximately five or six years ago we did have equipment which we modified and was released for sale to foreign governments and also to civilians.

Prior to 1960, it was known as Johnson Laboratories for seven or eight years.

So most of our expertise has been in the manufacturing of equipment, although we have done some countersurveillance work.

Now, we put a lot of effort into examining what was needed in the civilian area as far as technical security is concerned, mainly because, as I said, five or six years ago we did start selling to U.S. industry and law enforcement. We felt at that time we had to get some of this knowledge as to what the problem was, how sophisticated the attacks were on civilians.

So we do separate out two levels where we are concerned with the equipment and services, one being a governmental level and one being a civilian level.

MR. HERSHMAN: Mr. Daskam, I am glad you are here today, and I purposely put you with this panel because you have experience as a manufacturer as well as a user of the equipment.

May I ask, Mr. Daskam, what is your background, please.

MR. DASKAM: I have a Bachelor of Science degree in electrical engineering. I have been involved in electronics all of my career. I was an instructor for four years in electronics in the Air Force in the Bombardier-Observer-Navigator program in B-47s. And I am presently General Manager of Mason Engineering and President of the Technical Security Services that we have.

MR. HERSHMAN: Mr. Daskam, Mr. Nesbitt mentioned in his opening statement that in order to do a proper countermeasures sweep, one would need to possess equipment in the range of \$20,000. Do you agree with that?

MR. DASKAM: It is a little difficult to judge exactly what the value would be, but I would assume that that would be a ballpark figure, although I would think it might be less. I don't know exactly what Mr. Nesbitt uses now.

Here, again, you can't really get an estimate as to what equipment is necessary because some people believe in X-ray equipment; some people believe in metal detectors. But the two basic pieces we depend on are the radio receiver equipment and the telephone analyzing equipment.

MR. HERSHMAN: When you go out to do your search, how much equipment monetarily do you bring along with you?

MR. DASKAM: I would think it's around \$15,000 of equipment.

MR. HERSHMAN: Mr. Speriglio, would you tell us what equipment you use?

MR. SPERIGLIO: Yes. It varies depending on the nature of the assignment. On some assignments we bring out a limited amount of equipment in value probably \$3,000 to \$4,000. On very complex assignments we will bring out very expensive equipment. Recently we had to debug an answering service with 300 telephone lines. It required five of my agents working with every piece of equipment we had available.

MR. HERSHMAN: Could you give us an example of the types of equipment you use?

MR. SPERIGLIO: Most of the equipment we use is not equipment on the market, with the exception of the RF's. But most of our equipment has been built for us by our engineers or people we contract with. And it varies. It is very similar to the types that we previously described. I don't mean the black box operation, but from the telephone analyzers to the receiving equipment. It would take a long time to go into it piece by piece. I'd be happy to do it but I know time is short.

MR. HERSHMAN: How did you get into the countermeasures business? How did you learn how to do it yourself?

MR. SPERIGLIO: Well, pre-'68 in the State of California, bugging was legal, and as in most companies those days we performed electronic surveillance for certain clients, primarily to those businesses who suspected that they had dishonest employees, and there was a consensual recording law and we did quite a bit of it in those days.

By the same token, we were doing debugging. As a matter of fact, my agency goes back 70 years, and we have the first piece of bugging equipment ever used, from the turn of the century. There was even bugging back in those days, but not to the extent there is now.

MR. HERSHMAN: Mr. Nesbitt, could you describe to us perhaps the value of the equipment you use?

MR. NESBITT: Yes. The last one we completed we had a total evaluation on hand of approximately \$100,000, this was an exceedingly difficult one. One piece was insured for \$70,000. This is just the insured value. Another piece was a Hewlett Packard piece of gear—a spectrum analyzer. It costs around \$23,000, \$24,000, with no modification—we modified it.

MR. HERSHMAN: Do you provide checks at different levels for individuals?

MR. NESBITT: Yes.

MR. HERSHMAN: Would you explain to us what the levels include without going into the actual work?

MR. NESBITT: Well, I guess the best way to describe it would be that we use equipment in any basic search in the area of \$25,000. If we discover it is more difficult, we bring in the heavier pieces of gear.

I'd like to digress for one moment. Nothing was said in this hearing yesterday or today, and there is a technique, and I have developed and instructed government employees in its use, and that is a method that permits detecting devices on phone lines or communication lines far and above anything that has ever been shown here in the show-and-tell session.

But again, this involves time. It involves manpower, and it involves expensive equipment. But that is the ultimate.

And going down to the bottom, I'd say the bottom is about \$25,000 value of equipment.

MR. HERSHMAN: Tell me, Mr. Nesbitt, when you walk into a firm to do a sweep, do you guarantee the man—

MR. NESBITT: No.

MR. HERMAN: —that it will be 100 per cent sure?

MR. NESBITT: No. The reason for that is quite obvious. We can check and be fairly certain that his

phone lines and his facilities are clear. By the same token, no one can, we could literally take his place apart brick by brick and still not discover something. Or the adversary, if you choose to call him that, could be a very well funded adversary and be sitting across the street monitoring everything going on. And I don't want to go into that in open session.

MR. HERSHMAN: Mr. Daskam, considering that you have some of the best equipment available to you, how sure can you be that the sweep is effective? Can you give a percentage?

MR. DASKAM: I think you really have to break it down into three areas. One would be the radio transmitter. The second would be equipment used on the telephone line. And the third would be the wire and microphone.

With radio equipment, I feel reasonably sure on an industrial level—I am not talking about governmental level—you can be fairly sure you have checked every signal, and if you have been conscientious about it you can assure the people that there are no active transmitters radiating from that area.

On telephone equipment, there are certain devices which you cannot find on the telephone lines. And here, again, it is the thoroughness of your physical search when you follow up on this. And you are probably 99 per cent sure.

The very uneasy part comes with the wire and the microphone which is the most reliable and oldest of the devices. And here you are really relying on the effort of the physical search person, whoever it is, to really cover all the bases in looking for these wires. And your biggest risk area of not uncovering something would be during the physical search.

Now, if you want a percentage—I wouldn't even want to guess.

You always go away—maybe not at that instant but maybe the next day—saying really you should have taken one more thing apart or you really should have looked harder above the ceiling. You never come away, I think, with a complete feeling of 100 per cent.

What the percentage is I don't know. But obviously you are going to miss things.

Now, listening to various people give testimony—I am a little bit uneasy sitting here, because if you find 20 per cent of the jobs have bugging devices, I must be missing a lot of things.

MR. HERSHMAN: Mr. Daskam, I recognize you to be one of the most proficient men in the field in the country. You certainly have the equipment available to you to do a superb countermeasure sweep. Are you telling us you don't find as many as one bug in five sweeps?

MR. DASKAM: No. I'd like to explain something. We do a limited amount of this work. We really don't advertise it any more. At one time we felt there was a large amount of industrial business there. But because of the pressure of our manufacturing and engineering facility—we use the same electronic technicians, by the way, to do this work.

Now, we probably do between five and ten of these a year, but mostly for established customers whom we have done it for for several years.

As part of this service we don't go strictly into the technical security end of it. We also observe other weaknesses in security systems, physical security, paper work control. If they have shredders or scramblers, we evaluate these types of systems while we are there.

Now, we have never found an eavesdropping device.

MR. BLAKEY: Did you say never?

MR. DASKAM: Never.

MR. BLAKEY: In how many years?

MR. DASKAM: In four years. This is probably 40 to 50 jobs.

Now, we have found things which we don't know—we have found hot telephones where the audio always goes to the frame and this type of thing. But these devices—I don't want to say devices—these audio leaks, as we call them, can very well be accidental wiring or design failures in the telephone equipment. For instance, some types of telephone equipment have this event occurring.

We feel it is just as important we point out these weaknesses to the client as to actually find a device.

But as far as finding a device in the phones or in the room, we have never found one.

MR. HERSHMAN: Mr Nesbitt, could you give us a percentage of how many bugs you find? How long have you been in this business?

MR. NESBITT: Thirty years. It is more like two in 100.

MR. HERSHMAN: Well, do you have people working for you also?

MR. NESBITT: Yes.

MR. HERSHMAN: Well, do you have people working for you also?

MR. NESBITT: Yes.

MR. HERSHMAN: Two in 100?

MR. NESBITT: That is high.

MR. BLAKEY: This is using \$23,000 worth of equipment?

MR. NESBITT: This is using the finest we can get.

MR. HERSHMAN: How many sweeps do you do a year?

MR. NESBITT: I won't give you the exact amount but it's very high. That is our business.

MR. HERSHMAN: Approximately.

MR. NESBITT: Well over 100.

MR. HERSHMAN: Well, do you have people working for you also?

MR. NESBITT: Yes.

MR. HERSHMAN: How many people do you have working for you?

MR. NESBITT: Well, we have several thousand in the field. We are in the United States and Canada.

MR. HERSHMAN: Countermeasure technicians?

MR. NESBITT: In each office we have a chap.

MR. HERSHMAN: And how many offices do you have?

MR. NESBITT: Over one hundred.

MR. HERSHMAN: So I assume you do more than 100 a year.

MR. NESBITT: Yes. I am speaking from personal experience.

MR. HERSHMAN: If a device was found in Texas by your resident office out there, would you know about it?

MR. NESBITT: Yes, we would.

MR. HERSHMAN: So you could do thousands and thousands of these a year all told?

MR. NESBITT: And not find a bug. Is that what you are driving at?

MR. HERSHMAN: I'm driving at the incidence. That is what we are here today to try to find out.

MR. NESBITT: Yes, it is low by comparison to some of the statements made here.

MR. HERSHMAN: Do you feel you are over-looking bugs?

MR. NESBITT: No, I don't. But let me qualify that statement. And I can best graphically illustrate it this way.

We were doing a particular job in the New England states. While we were there we were checking the offices, and a pseudo-phone company employee presented himself to the main guard desk, entered with his tools hanging on his belt, and what have you, and had a clip on saying "Bell Telephone."

When we looked a little closer at a similar badge, we found the line, "Bell Telephone subscriber." There's a lot of those buttons around.

But we found several of those telephones had been third-wired, as we call it, a little hair wire jumping the cut-off switch. But this chap was rather breezy because he walked past the guard, back to the phone room, and managed to place several of the pilot lamps that you have probably heard mentioned on the five button set, that light up the push buttons, and he put them in these 66 terminals to jump over the phones that were wired to another line going out.

So this is the type of thing. It takes a thorough looking into.

MR. HERSHMAN: And you have been doing this for 30 years now? Is that right, sir?

MR. NESBITT: Yes. One other example I might just touch on quickly.

MR. HERSHMAN: Surely.

MR. NESBITT: Up in New England, also, we discovered a young couple having a fight with a local group, and everything they would say, and their friends would say, was being voiced elsewhere. We discovered that someone had put a line in right alongside of their existing phone line and not terminated it, merely inserted it in the box in their house and then out at the pole and elsewhere, and were recording everything being picked up from their phone line. It was in close proximity.

So there are a lot of things that are happening that can be explained away as an honest mistake by an employee but yet are suspect.

So I qualify my statement of one in a hundred because there are some others.

MR. HERSHMAN: One in five?

MR. NESBITT: No.

MR. HERSHMAN: Mr. Speriglio, could you tell us what the incidence of finds by your organization is?

MR. SPERIGLIO: They are a little different from those of my colleagues. This is strictly an estimation as we keep no exact records of this type of assignment. But since 1968 I would estimate our agencies combined—there are four of them—have conducted in excess of 20,000 debugging assignments that would probably amount to around 80,000 telephones and many millions of square footage which was checked for room bugs.

The percentage of find varies. I would say probably it is anywhere from 4 to 10 percent, and I will give a reason for that.

We are very selective in our clientele. If a client calls us up and says they suspect their phone is tapped because they hear clicks on their line, we tell them that is normally not a sign of wiretapping. If they report that there have been leaks that could have not left the office or resident phone by any other means, then there is a good chance that there is or has been a wiretap, and we will go out there.

I'd like to point out this, that 80 per cent of all our clients—and this includes a great number of attorneys—call us first on the phone they suspect is being tapped and ask us to come out and debug it. Normally, it takes an average of about three hours or more before our agents are able to arrive on the scene. And if the wiretap could be removed before we arrived there, the chances are we are not going to find it.

One more thing I'd like to point out, although this is not the exact question you asked, but I'd like

to answer it anyway, if I may.

As to what our agencies, namely Nick Harris Detectives and others, guarantee, the very first thing we guarantee our client is that if the wiretap originates in the central switching station of the telephone company, there is not any probability we are going to uncover it, and certainly the telephone company will not permit us to inspect their equipment. If the wiretap is in the telephone instrument, the likelihood is 99 percent it will be uncovered. For the majority of room bugs, we'd say the record of discovery would be quite high. On the telephone tap, if it is along the line or in other areas further away, naturally it is more difficult, and the percentage of finding or discovery reduces sharply.

MR. HERSHMAN: Mr. Speriglio, you are talking about 20,000 debugging jobs over the last seven years, and an average of 4 to 7 percent—let's say 5 percent finds, so we are talking about a thousand illegal devices. Can you tell me, sir, how many cases you have turned over to law enforcement?

MR. SPERIGLIO: None, and I will explain why. All our clients, including law enforcement and government agencies, do not want this information given out. Primarily companies—

MR. BLAKEY: Is it your testimony that not one of that thousand companies was willing to report it to the police?

MR. SPERIGLIO: With one exception, a recent case we handled, where the client was almost begging that we find a wiretap because it was involved in a privacy invasion lawsuit and it would strongly help her case. As it turned out, there was no wiretap. In this case, they wanted to turn it over to law enforcement. In all other cases, commercial or industrial, they want to keep these matters private.

We do fingerprint the bugs and, as you know, turning them over to law enforcement serves no useful purpose. Wiretaps have no serial numbers. They are not traceable and it is very rare a fingerprint would be found on them other than a smear.

MR. HERSHMAN: Do you mean you take the bugs into your possession?

MR. SPERIGLIO: We do one of two things, depending on who the client may be. Many times we recommend to the client to keep the wiretap in operation. The purpose of that is to feed false information to the adversary. Many times this may be trade secrets or bids or something of that nature, and it would be very important to feed false information to the other side as long as they don't suspect that our client has discovered the tap.

On the other cases we would either destroy the wiretap on the premises or leave them with the client. Occasionally, we will take them, with the client's permission, and use them for demonstration purposes in our training class.

MR. HERSHMAN: Do you consider that legal?

MR. SPERIGLIO: No, and I'd like to also point this out that according to the Safe Streets Act, the moment we remove a wiretap, physically touch it, we are in possession of a wiretap, and according to the statute we are in violation of the law.

MR. HERSHMAN: Do you feel that should be changed?

MR. SPERIGLIO: Yes. We know we are breaking the law but it's a borderline situation.

MR. HERSHMAN: I have a difficult time talking about the law knowing that there are 1,000 wiretappers out there in California walking around and those cases were never reported to law enforcement. It scares me. I just don't understand why this can't be done. I would think that as soon as a device is found it would be most prudent to contact law enforcement. And don't you feel you have a responsibility to report it to law enforcement?

MR. SPERIGLIO: It is not a question of responsibility. Under our state licensing, it would be in violation of our client's interest to report this to law enforcement. We are not permitted to, since our client is not involved in a crime, report this to law enforcement. As a matter of fact, we would be violating the rights of our client in the State of California.

MR. HERSHMAN: How would it affect your business if we mandated that you had to report a find to law enforcement?

MR. SPERIGLIO: It would affect the business. It would probably cost the client more money per assignment as it would create for us additional clerical work and possibly shipping the bugs wherever they might go, for storage or what have you. I personally wouldn't mind it one bit. As a matter of fact, I wish that we had better ways of protecting the privacy of the citizens of the United States, and I think it should be reported so we'd have some true figures as to how extensive wiretapping is.

I can tell probably from the tone of your voice, Mike, that you may disbelieve the number of finds or the number of assignments we have handled. And 1,000 bugs or wiretaps over a period of seven years have been found. The State of California is just one of the states in which we perform these services. Hundreds of thousands of wiretaps have been manufactured, as I pointed out in the manuscript you read, the earlier version of it. We have no idea how many—possibly millions of—various different types of bugging devices and wireless microphones, as they call them, and so forth, are available here in the United States. So if we just find 1,000, and we do the biggest percentage of debugging in the area—

MR. HERSHMAN: I sometimes find it hard to draw a parallel between the number of devices available and the number of wiretaps in the country.

MR. SPERIGLIO: Certainly if they are manufacturing them, they are not making one or two or three units. They are making a vast volume. If they are going to send out 1,000 advertisements every time, they must have quite a supply.

MR. HERSHMAN: Have you turned these advertisements you gave to us over to law enforcement?

MR. SPERIGLIO: The last ones I have not. On many occasions I have sent them to the Attorney General's office and also discussed this with the Federal Bureau of Investigation.

MR. HERSHMAN: Do you know of any prosecutions resulting from this?

MR. SPERIGLIO: The funny thing is they already have copies. They are apparently on the mailing list.

MR. HERSHMAN: What seems to be the problem? Do you get a feedback from the law enforcement agencies as to why they are not prosecuting?

MR. SPERIGLIO: To my knowledge, at least in the State of California, I am not aware of a single instance where a person has been convicted of violating the Safe Streets Act. As far as selling this bugging equipment, the loopholes in the '68 law permit this—as long as they are going to call it a burglar alarm or a baby sitter, or whatever they want to call it, under the guise of it being a purposeful service, it is legal for them to do it.

MR. HERSHMAN: Mr. Nesbitt, what is Pinkerton's policy as far as turning over illegal devices to law enforcement?

MR. NESBITT: I would say it's the same as I had all the years I was in the business. We subscribe to the law and express to the client at the very outset that should we find any devices, they must be reported to the Federal Bureau of Investigation because they are charged with the enforcement of this law.

MR. HERSHMAN: And is that the policy you follow?

MR. NESBITT: That is the policy we will follow. We will not touch a device. We tell the client and say they must call the FBI. We do not call because it is not our phone and not our business, but we strongly urge them to walk across the room and pick up the phone and call the Federal Bureau of Investigation.

MR. HERSHMAN: And what is their response?

MR. NESBITT: They are very glad to do it.

MR. HERSHMAN: So this has actually happened, then, where you have discovered a device and it has been reported to the FBI?

MR. NESBITT: I am certain of that.

MR. HERSHMAN: Do you know of any prosecutions resulting from any of the devices you have found?

MR. NESBITT: No, I can't say that I do. No, I knew a few things that were stirred up, but I don't know of any successful prosecutions because I don't follow them. I have other work to do.

MR. DASKAM: May I say something on that?

MR. HERSHMAN: Yes, Mr. Daskam, please.

MR. DASKAM: We have the same policy. However, when we first talk to a client, we make it very clear that he should have a top management decision on this as to how they are going to handle the situation. We tell them as far as our feeling is they should report it to law enforcement but they should make top management aware before they get involved in this whole thing that this is what should be done.

So we don't just leave it up to the security manager or personnel manager, or whoever happens to hire us, to make the decision. We say it really should come from the corporate management.

Another thing is it might be interesting—and I don't know if you know of this eavesdropping event that happened in Stratford, Connecticut, a few weeks ago. There was a device found there. I can't agree that turning over these devices to the FBI does no good. In any case, although I don't know all the events that have happened since then, I know the device was immediately sent to Washington, and it is my feeling that the FBI is the one who cracked the case as to who put the device in because they traced it as to who made it, and from that they were able to get the people who bought it. And it turned out to be two local policemen who installed it in Town Hall.

I can send you that information if you like.

MR. HERSHMAN: I would appreciate that, Mr. Daskam.

MR. DASKAM: It might be worthwhile following that up to see exactly how the sequence of events was handled as far as getting that information.

MR. HERSHMAN: Yes, Mr. Nesbitt.

MR. NESBITT: I'd like to add we have had very fine rapport with the Bureau and other agencies, and we work very closely with them, and for over 20 years I worked exclusively for the federal community, up until 1966. We have had nothing but the finest cooperation in anything we had to undertake, but we don't feel it is up to us to take it to the Bureau. We tell the client who hired us to tell them.

MR. HERSHMAN: Mr. Speriglio, are there charlatans in this field of countermeasure services?

MR. SPERIGLIO: Unfortunately, yes. As in many professions, there is always a bad apple. In this case, there is a big bushel of apples, and most of them are bad. There are professionals here at this time, and many of my colleagues throughout the United States are very professional and they are not charlatans or black box operators. But there is a great number of them.

MR. HERSHMAN: Can you give us some examples of individuals in this business that are in it for the primary purpose of ripping off the public?

MR. SPERIGLIO: Yes. From what I have been told, they have business cards, in most cases not even a city business license. They solicit more or less on a door-to-door basis to companies. The companies now are so paranoid anyway that they think their phones are tapped or their rooms are bugged, and in many cases they receive the assignment. Their fees generally are fairly low.

And I will give you a quick for-instance, if I may. I was attending a law enforcement party sometime back and during the course of the party we were discussing the black box operators. And during that time one of the law enforcement officers produced a recording, a tape recording, and we got to hear a portion of it. It went something along the line as I will state.

The black box operator finished telling the client, "Mr. So and So, your premises have been completely cleaned. My black box has never been wrong"—he didn't call it a black box—"and there are absolutely no bugs or wiretaps."

And the client said, "I really feel great about it. Now I can really rest at ease feeling my premises are clean."

Of course, everybody at the party had a big laugh.

MR. HERSHMAN: Mr. Speriglio, you have a rather large private investigative firm. How often do you receive calls to engage in illegal wire-tapping?

MR. SPERIGLIO: On an average of three times a day. It varies. Some of the calls are actually from legitimate clients. Others are either from law enforcement bodies or competitors to keep us in line, to make sure we are not taking any bugging assignments.

MR. HERSHMAN: Can you tell us if some of these individuals calling you and asking you to do bugging or wiretapping ever explain why they want it done?

MR. SPERIGLIO: Oh, yes.

MR. HERSHMAN: What are some of the reasons, please?

MR. SPERIGLIO: Many times they feel it is perfectly legal for them to do this. It is their premises.

They feel that they should have the right to have a recording of whatever goes on in their office or business. They might explain that they are going to be involved in a meeting where they want to have a recording of it.

It may be a domestic situation where a spouse wants to record the other spouse if he is leaving town and check on the phones in the bedroom.

They vary. And, of course, we receive all sorts of requests.

MR. HERSHMAN: What do you charge for your countermeasure services?

MR. SPERIGLIO: That, of course, varies, depending on the complexity of the assignment. We have a minimum fee of \$150. The charges are based on the type of telephone equipment, such as touchtone, direct dial, PBX boards. It is based on square footage. The rates increase and decrease depending on the number of instruments, the number of square footage involved, the location.

MR. HERSHMAN: Can you give us an average?

MR. SPERIGLIO: I would say the average debugging would run from \$350 to \$750. Some run into many thousands of dollars, but it depends on how complex they are.

MR. HERSHMAN: Mr. Nesbitt, have you ever been asked to perform a countermeasure service by a member of organized crime or someone who is fearful of being eavesdropped on by law enforcement?

MR. NESBITT: Not knowingly. The point that I make is that if organized crime wanted it, they have the funds, I am sure, to do it themselves or they'd get someone. And I don't think they'd be the ones to tell us that they are organized crime. And we, fortunately, deal only with legitimate businesses. And earlier I heard the phrase, "the Fortune 500." We have a few clients in that group.

MR. HERSHMAN: Mr. Daskam, have you found there is an increased interest on the part of organized crime or other criminals to purchase the equipment you manufacture?

MR. DASKAM: I know they are interested in it but the price of our equipment seems to not be attractive to them and they go to less expensive equipment.

We have inadvertently done one job in New York City where it was a single technician that went down, but it was under a manufacturing company's name, and he ended up out at Long Island out at the estate. And it was a rather unfortunate situation.

We tend not to do individuals. We try to stick with corporations which we know, and if we had known what situation we were getting into there, we'd have turned it down.

One thing came up before on the organized crime thing.

I don't know. It is difficult to tell sometimes when people call up. They are a little reluctant to tell you right away who they are. But usually we insist on knowing the background and where the locations are.

I don't think that they are any more concerned about it than anyone else. They tend to have better physical security, I think, than most people. They know who should be in various locations and who shouldn't be. They are more concerned, I think with undercover agents than wiretaps.

MR. HERSHMAN: Mr. Speriglio, when I had occasion to interview you on the West Coast, you had mentioned that sometimes you call other private investigators in order to determine whether they will provide offensive wiretapping and bugging operations. What have you found out in the Los Angeles area?

MR. SPERIGLIO: Well, a small percentage—generally the agencies that are willing to provide the service—normally it is either a one-man operation working out of his garage or residence. I have never found any large companies such as Burns, Pinkerton, or any of the major ones that will offer to do this. We don't even call Pinkerton's, by the way.

MR. NESBITT: Thank you.

MR. SPERIGLIO: I'm sorry for that. But in the State of California, we have approximately 5,000 investigators either licensed or operating under the license of a licensee. We certainly don't call them all, but we spot check them or certainly the new ones that come in, or any time we see ads in newspapers providing services—similar to what took place earlier on the tape recording you had on another matter.

You'd be surprised. We had one agency who not only offered to do a wiretap for us but agreed to do a kidnapping at the same time.

MR. HERSHMAN: How long ago was this?

MR. SPERIGLIO: That particular one about a year ago, and it was in the city of Glendale.

MR. HERSHMAN: Yes. And they offered to do a kidnapping?

MR. SPERIGLIO: We pretended to be Dr. So and So. We wanted him to break into the wife's house and take the child and at the same time plant some eavesdropping equipment so we could get evidence for the child custody. And he agreed to do it.

MR. HERSHMAN: What are the licensing requirements in the State of California for a private investigator?

MR. SPERIGLIO: They are very strong. They require a minimum of 4,000 hours training preliminary to taking the written examination for a license. They are very thoroughly checked out. New York and California have the strongest requirements. The bond is just \$2,000 in California, where in New York it is \$10,000. We carry \$1,300,000 liability insurance, which is not required.

MR. HERSHMAN: But even with the strict licensing requirements, from what you have just told us, it doesn't seem to keep the illegal operators out.

MR. SPERIGLIO: Well, again, we are talking about a handful. There are 5,000 investigators and approximately 15 to 20 do this, which is a very small percentage. You will find a percentage of corrupt persons in anything. You have that in politics, too.

MR. HERSHMAN: Mr. Nesbitt, earlier you mentioned that there is a necessity for you to carry or possess surreptitious interception devices. Why is that?

MR. NESBITT: Very simple. In holding the seminars for law enforcement and industrial persons, we have to show them the devices and give them some indication of what they should look for, how to cope with this. We do show them what they can look for.

MR. HERSHMAN: And so you feel it is necessary in order to teach countermeasures, to show the devices; is that correct?

MR. NESBITT: Let's not have any misunderstanding. We are not teaching countermeasures per se. We are merely, in a seminar, offering the explanation of what they are faced with and what they can do to help combat it. We are not training people to be countermeasures experts—no way, by no stretch of the imagination.

We do have very qualified countermeasures people from police departments, even foreign police departments, that come and take advantage of this so that they are kept abreast of the problems that are being faced on a daily basis. That is the purpose of the seminar. And that is why I take these devices with me, in a little locked case, but I do feel under the law there should be some provision for this.

I will say this, and the Lord can be my witness on this—and others will. I have been in this business for years. I have built and delivered to the federal community—I have never sold to the private community—many thousands of dollars in devices, but I have never used one in my life—never. And that is a very, very important statement. I am against the use of bugs, and I enjoy my work tremendously in trying to counter them.

It is an ongoing problem, but the thing is growing every day and getting more exotic. The type of things mentioned here and shown in the show-and-tell session are just the tip of the iceberg.

MR. HERSHMAN: As you know, Mr. Nesbitt, we are currently doing a state-of-the-art technology study, so we may bring Congress and the President up to date on the latest advances in technology.

MR. NESBITT: Yes.

MR. HERSHMAN: How effective, really, can a countermeasures search be if the minute you leave the swept area a device can be planted?

MR. NESBITT: Mr. Hershman, you answered your own question, I think. It is very poor as an overall effort, if the client has no control over egress and ingress. Five minutes after we leave somebody could plant something. As I said earlier, though, it is not necessary to gain access to do this type of thing.

MR. HERSHMAN: What do you charge for your countermeasure services, Mr. Nesbitt?

MR. NESBITT: We have a rate of \$50 per man-hour. We have a minimum of two men per job. And there is a reason for that, other than psychological—a minimum of two people on the job can conduct a thorough search. That is a minimum. So it has turned out to be \$100 minimum.

MR. HERSHMAN: Mr. Daskam, how do we drive the charlatans out of this business?

MR. DASKAM: I don't know. I am going to have to write you a long letter on that, I think, after some careful thought.

You know, it may seem that licensing will be the cure-all, but I think we are going to run into situations here similar to what we have with private detectives. Because as soon as the situation comes up where someone is not aware of the licensing requirements they are going to be doing it. And once they get that type of business, it will just grow. It is going to be very difficult to do.

MR. HERSHMAN: On the other hand, Mr. Daskam, if I may interrupt for a second, if we do license competent people, won't the public have a body to draw from on which they can rely?

MR. DASKAM: If the public knows this. But the problem—you asked the other gentlemen here if they get calls requesting people to install these devices. We get calls like this. And I think maybe in a year we may get 40 or 50 calls. Perhaps one person knows that it's illegal out of the 40 or 50. The balance of them are either in retailing or manufacturing, and they have an internal problem which they are trying to control.

I will give you some instances. We had a call a few weeks ago from someone who is concerned because people are going through the cash register

in a discount store when a friend is at the cash register. They ring up \$1.50 when they have \$20 of merchandise in the bag. He wanted to install transmitters under each cash register so they could listen to the people they suspect of this. We said that was illegal under the Safe Streets Act, and they had no idea it would be illegal.

One, if you are going to have licensing, there has to be some way of education so the people will know that qualified or licensed people are available. They know this on private detective agencies because every state has laws on that.

Now, perhaps this is where the effort may come in, that there is some type of local control on it because I don't think the Federal Government really has enough eyes to watch this type of situation.

We find this with eavesdropping device manufacturers.

MR. HERSHMAN: So what you are saying, perhaps, is we could recommend the states enact regulations.

MR. DASKAM: Maybe it has to be tied in with LEAA grants. You know, if you don't have this kind of law you don't get the money for this. This is done regularly under federal grants, where they have these provisions on safety requirements on highways. If you don't have certain standard requirements on highways, you don't get the highway funds.

Perhaps that is the way to go, which makes more sense. Put the onus on the state to control this type of thing because they already have the licensing set up for private detective agencies.

MR. HERSHMAN: Some states do.

MR. DASKAM: I don't know. You may be right that some do and some don't. And, of course, the problem is if you let the states set it up, some get very slipshod on requirements.

MR. NESBITT: I want to correct one thing. You probably recall about two years ago in the *Wall Street Journal* there was quite an extensive story on a police officer in the Midwest who had retired from the force and was now becoming a countermeasure expert and was a millionaire; he was charging \$600 a room to do this. He was using one of those \$29.95 detectors and was getting around and giving this false feeling of security; the problem is—and I don't envy you folks on the panel this chore, but it is purely an educational problem of the public. In time of stress, where does one turn when he needs help? The first is to the man who is privileged to wear the badge and the suit of blue, the police officer. He has human frailties, and these are found in every other field. There is this one chap who had resigned from the force and now is

making many, many more dollars than he made as a police officer.

MR. HERSHMAN: How do we get them out of this business?

MR. NESBITT: That's the point I'm making. It is a problem I can't solve. I don't know how to do it except for a very stringent licensing law for the manufacturer of and the use of such equipment.

MR. HERSHMAN: Mr. Speriglio, do you have any ideas along this line?

MR. SPERIGLIO: Yes, a thought just came to my mind as you were speaking. Supposing a law is passed requiring registration and licensing of a countermeasures expert. What good is it going to do when the telephone companies won't let you advertise in the phone book anyway?

MR. HERSHMAN: I suggest if we have strict licensing and can assure the public of competent services, I think the telephone company would probably be agreeable to running ads.

MR. SPERIGLIO: Do you really think the telephone company would be happy having people finding taps allegedly planted by the phone company?

MR. HERSHMAN: Excuse me.

MR. SPERIGLIO: Do you feel that the telephone companies would really allow in the yellow pages a service to detect telephone taps even if it might be one of theirs?

MR. HERSHMAN: You are suggesting that the telephone company is tapping phones? If you are suggesting that, I ask you to offer the evidence at this point, the proof.

MR. SPERIGLIO: There has been plenty of evidence which has come to recent light. One man mentioned earlier today the AT&T monitoring 30 million telephone conversations. They actually recorded 1.5 million of those phone calls, and their purpose was to find apparently 200 violators of toll calls.

Why would the phone company really want to go at random to check 30 million phone conversations?

MR. HERSHMAN: So it is your contention that the reason the telephone company is keeping the countermeasure services out of the yellow pages is because they are afraid you people would discover their bugs?

Didn't you tell me recently, Mr. Speriglio, you couldn't detect a telephone company tap if you wanted to?

MR. SPERIGLIO: This is not counting taps that a telephone lineman could put on the line.

MR. HERSHMAN: Why would the telephone company use a lineman to do it when they could do it without anybody being able to observe it? It doesn't make sense.

MR. SPERIGLIO: It makes sense. It is just a question of how they want to employ the tap and the purposes of it. It has been alleged—I am citing now a Texas case recently. I believe it is Southwestern Bell. The panel may know it and I need not go into it. But they were reporting the telephone companies were tapping telephones and the tapes were coming out in barrels each day.

MR. HERSHMAN: Still, if the telephone company were going to tap a telephone, it would only be reasonable that they'd do it in a manner which would leave the littlest room possible for discovery, and that would be at the central frame. So I really don't agree with your argument that they are keeping the advertisements out of the yellow pages because they are afraid that people are going to discover their taps or bugs.

MR. SPERIGLIO: Let me answer this with a letter from the Public Utilities Commission and a reply from the telephone company. It states:

"In December 1971 our company revised its standards for yellow page advertising content pertinent to the classified heading of 'Detective Agencies and Investigators,' specifically, and all classified headings in general. This was done in an effort to comply with the intent of the federal Safe Streets Act of June 1968. The standard not only prohibits the advertising of wiretapping and eavesdropping devices but also so-called debugging advertisements, on the basis that those who can debug also possess the capability to bug and wiretap."

Now, that is a lot of nonsense. I am sure you, Mike, as an expert, know almost anyone can perform a wiretap. My three-and-a-half year old daughter did in 28 seconds. We took a picture of her for my book, putting in the drop-in transmitter.

MR. HERSHMAN: We are talking about two dif-

ferent things. I don't know if I agree with the telephone company policy. What I disagree with is your statement that they are doing it so their own taps won't be discovered.

MR. SPERIGLIO: I am not saying that to libel myself. I am saying if that is not the reason, what is the reason?

MR. HERSHMAN: I think we will get the answer tomorrow because the telephone company is appearing before us.

MR. SPERIGLIO: I understand that. I read in the newspaper a quote from you, I believe, that Pacific Telephone admitted to discovering somewhere in the neighborhood of 1,000 telephone taps.

MR. HERSHMAN: The telephone company has given us data showing us how many illegal devices they have found over the last seven years.

MR. SPERIGLIO: During my investigative study for research on the book, that same source reported to the national press and to myself from the Chief Special Agent's Office that they discovered a total of 24 wiretaps. That was just last year.

MR. HERSHMAN: All I can say is that the information we saw from the telephone company was given to us under subpoena and whatever discrepancies there might be—

MR. SPERIGLIO: Was this AT&T on the whole or just Pacific Telephone?

MR. HERSHMAN: We have a breakdown on all the subsidiaries of AT&T.

MR. SPERIGLIO: Because Pacific Telephone did come out from the Chief Special Agent's Office with only 24.

CHAIRMAN ERICKSON: Chief Andersen.

MR. ANDERSEN: I have no questions.

[Material relevant to the above discussion follows.]

Catching spies in industry now a big business itself

By Colin Dangaard

A quality-control worker in a dog-food plant bugs a telephone, learns the formula for the most popular line, takes it home and starts his own successful company.

A man dressed in plumber's overalls sits on the roof of a building and aims a high-powered laser beam across the street, through a plate-glass window and into the conference room of a large construction firm planning a bid on a \$4 million bridge.

A janitor installs a "spike mike" in the washroom off the chairman's office in a biscuit factory, and a girl setting hair in a fancy salon gently questions the wife of an automobile company executive.

And while a beautiful blond who can't type schemes to become secretary to an industrial chemist, a burglar with a spy camera spends Sunday in an electronics plant photographing documents marked "Top Secret."

IT'S CALLED industrial espionage and experts say it's costing the United States \$6 billion a year.

Trade secrets taken from the Monsanto Chemical Co. in Chicago recently by two men were valued in the multimillions. They were turned in when they tried to sell them to the Stauffer Chemical Co. for \$5,000.

A former employe of Procter and Gamble was caught when he tried to sell his company's entire promotion program for Crest toothpaste to Colgate-Palmolive for \$20,000. It was valued at \$1 million.

Many companies go broke before they find the leak in secrets. One Los Angeles firm lost \$500,000 in sales in 90 days because of a stolen act.

THUS, A NEW INDUSTRY has been born: counterespionage.

Which brought us to Milo A. Speriglio, 38, tall, with heavy, strange-shaped glasses. He was sitting at a gigantic desk in a spacious office high above the Los Angeles smog. There is an adjoining steam room; the suite includes a cocktail bar, and a putting green is laid out on the carpet.

Speriglio smiled. He is director and chief of Nick Harris Detectives Inc., the second largest company of its type in the country. His time costs the corporation "around \$55 an hour." He lives in a luxury home with a young family and drives a Silver Mark IV which, he adds, "is about all I have in common with Cannon."

A spy for the good guys, Speriglio's main preoccupation is catching the bad guys' spies.

"Americans," he said, "are now spending more money spying on each other than they are spying on other countries."

THE SECRETS WAR down at the plant is getting dangerous as well as hot. Speriglio has been shot at and threatened with death and lifts the phone at least once a week to answer questions on what it would cost to break an arm or a leg or even do a complete rubout.

"We quickly explain," he said, "that we are not in the business of breaking bones. Just theft."

Several recent spies turned up by Speriglio were beautiful prostitutes retained by one company to pass themselves off as secretaries inside another.

"Pretty soon," he said, "they had worked their way onto the boss' couch and into his filing cabinets. In a couple of cases when the girls learned a certain amount of classified information, they revealed who they were and got other secrets by blackmail, threatening to talk to the wife, not to mention the stockholders, about their little 'affair.'"

INDUSTRIAL ESPIONAGE is a war of technology as well as people. Speriglio has a gadget, called the Nick Harris Sweeper, that can dial a number on the other side of the world and reveal a tone-activated bug.

"It cost us \$38,000 to develop," he said, "but the parts are worth only a couple of hundred dollars and can be assembled by a reasonably expert technician in several hours."

His agents often work in vans fitted with any one of some 200 magnetic signs he carries in "stock." They park outside buildings for days, sometimes weeks, filming through one-way glass, taking notes, eating and sleeping in an area the size of a small washroom.

"After one of those assignments," said Speriglio, "we automatically give the men three days off. When they step out, they can barely walk."

COMMERCE HAS BECOME so structured, and business so keen, that today it's often possible to take over a whole company simply by taking possession of its secret.

As demand grows for spies, so does their price.

"Six or seven years ago," said Speriglio, who has been in the business since he was 20, "you could get a room bugged by a private investigator for about \$300. Now the going rate is from \$5,000 to \$25,000."

ALTHOUGH THE SPIES contend they're selling risk — since it's no longer legal to tape-record a conversation without consent of all parties — Speriglio insists industrial espionage is the safest, highest-paying crime available.

"Go out and rob a bank," he said, "and the chances are you might get \$200. But then you have to shoot your way through the local police and spend the rest of your life ahead of the FBI. Do an industrial spy job and you're going to make yourself \$5,000 or perhaps \$20,000 in a month or less."

"If you get caught, nobody stops you with a bullet or a jail sentence. The worst they'll say is, 'Don't let us catch you on these premises again.'"

In California, for example, there is only one statute covering the theft of trade secrets—499C of the Penal Code. In many states there is none at all.

Said Dist. Atty. Phillip Halpin, a member of the major-frauds division for two years, "I reject more cases than I prosecute because they fall short of 499C. There's only a small body of law on industrial espionage. It's a new, unsettled area."

SPERIGLIO CALLS Los Angeles "the industrial spy capital of the world," with its large concentration of manufacturers, its vast business flow and its strong international connections.

The spy often hangs out in bars and private clubs frequented by industry chiefs. Simply overhearing somebody complaining that he wished he knew what so-and-so was going to do next could afford introduction.

Speriglio said businessmen will typically make a deal to pay on receipt of secrets, seldom wanting to know how they will be stolen, or even who will do the stealing. Some spies first get possession of the secret, then "shop around" for a buyer.

Bug planting remains popular. Sweeping offices for fees ranging upward from \$20 a time, Nick Harris agents have found bugs in telephones, furniture and, in one case, imbedded in the soil of an indoor plant — a "welcoming gift" from one company to a new competitor.

TO CATCH A GOOD SPY you need a slightly better spy. So Speriglio starts apprentice investigators at \$11,500, moving them, 2,000 hours later, to staff investigators at \$23,000 and (with 8,000 hours' experience) to a salary of \$30,000, with full expenses, including cars and phones. He has 270 agents in Los Angeles, and 427 associated offices around the world.

Speriglio has seen a lot of changes in the spying business, since his first job with the City of Los Angeles investigating applicants for civil defense. But he forecasts many more to come. "It's going to get a lot more vicious before it gets better," he said.

THE GEORGE WACKENHUT Corp. of Florida, the third largest industrial security organization in the nation, has doubled its business in the last four years. Public relations chief Don Richards said the company now employs some 18,000 persons, mostly guards, and has branches in England, France, Italy, Canada and four countries in South America.

The growing need to protect industrial secrets is given as a major cause for this rapid expansion. In Los Angeles, private investigators, most of them involved with industry, fill five Yellow Pages in the phone directory.

So voluminous has business become that they can now specialize. With Keith Rogers, for example, it's undercover. He employs some 50 agents who function as counterspies in every place from biscuit factories to electronics plants. He recently paid an agent \$700 a week to identify an electronics engineer stealing secrets in a components factory.

"The best qualification for the job," he said, "is an ability to keep your mouth shut. You just can't afford to get caught working

undercover in a factory. Too easy to have a bundle of steel drop on your head, or find yourself locked in a cold room. Bad undercover agents have a habit of disappearing."

JOHN C. HALL, owner of Securities Unlimited, was called to another state recently to bust a ring of people swapping horses in a breeding scheme. In the Lake Tahoe area of California he flushed out a spy selling client-list information from within a multimillion-dollar real-estate development.

John L. Kelly, former deputy regional director for the U.S. Bureau of Narcotics and Dangerous Drugs, recently found a bug in the office of a fabrics dealer who couldn't understand why he was constantly underbid on contracts.

"He was going broke," said Kelly, who discovered the bug in a telephone conference terminal on the director's desk. It took him two hours. He followed the wire through an air vent to another office in the same building.

The room was empty.

"The spy heard us coming," said Kelly.

EDWARD GLEB OF INTERCEPT believes in catching the industrial spy at the front door. He specializes in lie-detector tests for staffs of entire corporations, with particular attention to new employees.

He is confident the polygraph is "between 97 and 98 per cent" effective in identifying potential spies, including government inspectors.

Has he found any federal agents? "We're not saying."

Bug-finding: lucrative business

By Clarence Page

IT CAN be as small as a matchbox and easy to make as an old crystal radio set. In simplest form, it's a miniature FM transmitter with an evil name: "bug."

Fear of bugs and wiretaps, both of which ~~are illegal unless~~ backed by a court order, has brought lucrative business to private detectives like Edward R. Kirby & Associates, Oak Park, who last week found evidence of four in operation around the state Capitol in Springfield.

Or to private eyes like Anthony Pellicano, of Westchester, who found a microwave transmitter two years ago in Secretary of State Michael Howlett's office.

PELLICANO, whose more recent cases have included finding artist Yoko Ono's missing son and scrutinizing Rosemary Woods' 18-minute tape gap, says the Watergate era has been very good to the surveillance business.

"I'd say bugging and wiretap equipment manufacturers are doing at least 50 per cent more business since Watergate erupted," he said.

Electronic eavesdropping without a court order and the sale of equipment have been illegal in the United States since 1968, but that doesn't stop the nosy. Some perfectly legal devices, such as small FM transmitters used by housewives to monitor their nurseries, can be easily utilized for clandestine purposes.

Springfield and Chicago offices and his Crystal Lake home.

They detected four bugs operating within a two-to-four-block radius of the Capitol "and possibly within the Capitol itself," Lindberg's security chief, Roger Nautrt, said.

Gov. Walker asked Clarence Kelley, Federal Bureau of Investigation director, for a "prompt and thoro investigation" of the reported Springfield bugs. The Illinois Senate adopted a resolution the same day calling for a new legislative committee to investigate electronic eavesdropping.

Nauert said the search was halted after no bugs were

found in Lindberg's office. But other countersurveillance experts say the data could have been more specific.

"It's a fake," Pellicano declared. "If there was evidence of frequency transmissions, they should have been able to pick up the conversations, analyze the frequency and strength and pinpoint absolutely where they were coming from without any trouble."

WHEN ASKED about these techniques, Nauert said the varying thickness of walls made it impossible to determine the exact location without entering private offices or apartments.

MORE ELABORATE devices can dodge jamming by rapidly shifting signals thru a range of frequencies every second. It can only be decoded by a similarly sophisticated device.

"You couldn't find a bugging device small enough to squeeze into a martini olive like they do in the movies," said Eugene Allen, of E. V. Allen & Associates. "But we're coming close."

Sangamon County State's Atty. C. Joseph Cavanaugh launched an investigation Wednesday after George Lindberg, state comptroller, hired the Kirby agency to check his

CHAIRMAN ERICKSON: Gentlemen, I certainly want to thank you for what you have offered today. I think we are in a field that is complicated. I think it is, as has been said, the tip of the iceberg, the paranoid conclusions we all have that we are all being eavesdropped on at one time or another.

I think that the intent behind the Omnibus Crime Control Bill was to offer a means to regulate this rather complex field, and I hope we can make some

recommendations that will carry out the intent of the Act.

Thank you gentlemen, for appearing. We stand recessed until 9:30 tomorrow morning at which time we will reconvene in a different room, Room 1318, in this same building.

[Whereupon, at 5:30 p.m., the hearing was adjourned, to reconvene at 9:30 a.m., Friday, June 27, 1975.]

Hearing, Friday, June 27, 1975

Washington, D.C.

The hearing was reconvened at 9:30 a.m., in Room 1318, Dirksen Building, William H. Erickson, Chairman, presiding. Commission members present: William H. Erickson, Chairman; Richard R. Andersen, G. Robert Blakey, Alan F. Westin. Staff Present: Kenneth J. Hodson, Esq., Executive Director; Glenn Feldman, Esq., Michael Hershman, Esq., Milton Stein, Esq.

PROCEEDINGS

CHAIRMAN ERICKSON: Ladies and gentlemen, pursuant to the usual pattern of our Commission we are going to start on time.

The first witness this morning is Mr. James S. Reynolds of the Department of Justice, and we are particularly pleased to have him with us.

James S. Reynolds has been assigned to the Protection of Government Operations and Property Unit of the General Crimes Section since July of 1973. That unit is responsible for enforcement of criminal sanctions against wiretapping and electronic surveillance. Since September 1974, Mr. Reynolds has been in charge of the unit.

Mr. Reynolds, will you come forward and be sworn?

[Whereupon, James S. Reynolds was duly sworn by the Chairman.]

CHAIRMAN ERICKSON: Mr. Hershman will commence the inquiries following an opening statement, which I believe you have.

MR. REYNOLDS: Yes, sir.

CHAIRMAN ERICKSON: As I understand it, you are filing your statement, and all of the documents that you have tendered will be filed and made a part of the record, but we would appreciate a summary of your opening statement.

TESTIMONY OF JAMES S. REYNOLDS, ATTORNEY, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE

MR. REYNOLDS: Let me say, Mr. Chairman, that I appreciate the opportunity of being here this morning. Those of us in the Department of Justice who are involved in the enforcement of the sanctions against illegal electronic surveillance have enjoyed the opportunity of working with Mike Hershman and other staffers of the Commission and we

look for good things to come out of the work of the Commission.

The area of interest that I have this morning, of course, centralizes in the criminal sanctions against illegal electronic surveillance which, as this Commission knows, are basically contained in Sections 2511 and 2512 of Title 18 U.S. Code. Section 2511, of course, prohibits the interception of communications while Section 2512 governs the availability of devices primarily useful for the surreptitious interception of communications.

Our experience indicates that most violations of Section 2511 fall into one of five general categories:

First, domestic relations which we define to include intercepts incident to relationships between husband and wife, parent and child, and paramours;

Second, industrial espionage;

Third, political espionage;

Fourth, law enforcement; and

Fifth, intrabusiness which we define to include intercepts incident to dealings between labor and management, a business and its customers, and rival factions of management or labor.

The vast majority of violations which come to our attention are in the domestic relations category. You can see this from the statistics which have been generated through an inquiry by this Commission. The FBI has advised the Commission that over the past 8-1/2 years it has received something slightly under 500 reports of wiretaps from AT&T affiliates. In most of those incidents, the ensuing investigation has revealed an apparent motive for the wiretapping activity. Focusing on the cases where such a motive was developed and rounding off to the nearest one-half of a per cent we find that 80 per cent of those cases were domestic relations; 2 per cent were industrial espionage; one-half of one per cent were political espionage; 1 per cent were law enforcement; 5 per cent intra-business; and 11 per cent involved other motivations, the most common of which were theft of service and adolescent mischief or experimentation.

The Department's over-all prosecutive policy under Section 2511 has been to focus primarily on the professional wiretapper or the person who engages in or procures wiretapping as part of his profession or business activities. This makes our primary targets private investigators, attorneys, law

enforcement officials, business executives, and politicians. Less emphasis is placed on the prosecution of persons who, in response to a transient personal problem, intercept communications on their own without the assistance of a professional.

The development of prosecutable cases under Section 2511 is generally difficult, due to the inherently clandestine nature of interception activity. Interception devices discovered in place are surprisingly often not traceable as to where they came from. Absent some fortuitous circumstance, such as a violator being observed installing his device, it is frequently impossible to build a prosecutable case without the assistance of one of the violators. In this regard the immunity power is certainly of assistance, although we are reluctant to use it unless we first develop some independent evidence that will prevent the witness from taking all the blame upon himself thereby exculpating other persons involved.

In domestic relations violations you have a compounding of the investigative problems with certain prosecutive problems. We find the victims of domestic relations electronic surveillance very frequently unwilling or hostile witnesses on behalf of the government. Apparently they fear that facts about their personal life will be dragged into the courtroom. In instances where we try to prosecute one family member for the interception of communications of another family member, we have a difficult time meeting the high standard of criminal intent embodied in the statute. The Fifth Circuit decision in *Simpson v. Simpson*, 490 F. 2nd 803 (CA5, 1974) which we feel is incorrectly decided, has had the effect of extending the criminal intent problem to domestic relations electronic surveillance cases involving attorneys and private investigators. Finally, we have encountered what we consider a surprising amount of judicial distaste for domestic relations oriented prosecutions. Some Federal District Court judges have expressed doubt as to whether their court is the appropriate forum and a felony prosecution the appropriate medium for handling such cases. We have received pressures from judges to dismiss cases outright, to accede to *nolo contendere* pleas, to dismiss in favor of guilty pleas to inapplicable misdemeanors and dismiss in favor of state misdemeanor prosecutions.

Despite these problems, we feel Section 2511 is basically a soundly-drafted, viable statute. Through some minor changes to the existing framework of the statute these difficulties could largely be alleviated. We discuss at some length suggestions for possible legislative changes in the written statement which I have submitted to the Commission. I would simply say at this time that we feel it is imperative

that a misdemeanor with a reduced standard of criminal intent be added to the statute and that consideration should also be given to the adoption of a strict liability civil penalty.

Turning for the moment to Section 2512, we feel it is, in conjunction with Section 2513, a useful tool in limiting the availability of devices primarily useful for surreptitious interception of communications. However, the statute is simply not designed to prevent the distribution of all devices which may be of assistance to wiretappers and eavesdroppers. Further, it appears that a proscription of all such devices would not be feasible without it also having the effect of prohibiting the manufacture and possession of many normally innocuous electronic devices which are in common usage today.

I would note in this regard that most of the violations we encounter of Section 2511 are perpetrated with a device not prohibited by Section 2512. Accordingly, in our view, the best approach to curbing the availability of electronic surveillance devices rests in making Section 2511, the use provision, a more effective prosecutive tool. If the risk is made great enough, the market for interception devices will dissipate. To create such a risk, however, the Department needs not only some changes in Section 2511, but also very importantly—and I can't stress this too much—we need the assistance of state prosecutors in shouldering part of the load of enforcement of this area of the law.

Thank you.

MR. HERSHMAN: Thank you, Mr. Reynolds.

Mr. Reynolds, in your opening statement you mentioned there is currently one case involving the interception of oral communications pending under Section 2511 (1) (a) of Title 18. Could you tell us the circumstances of that case?

MR. REYNOLDS: It is *U.S. v. Burroughs*, a case out of the District of South Carolina pending in the Fourth Circuit. It involves an interception of oral communications by the representatives of a large national textile firm, who were seeking to overhear the communications of union organizers.

It is an interesting case because of the constitutional issue and also as to the sophistication of eavesdropping which is generally encountered by the Department of Justice. First, the legal problems that have been encountered in the case: We initially charged the case under 2511 (1) (b) (1) to avoid the constitutional issue involved in the charging of oral communication intercepts under Section 2511 (1) (a). However, as we looked at it we weren't sure the device met the criteria for 2511 (1) (b) (1) so we decided to recharge. We could have recharged under 2511 (1) (b) (4) and still have avoided the constitutional issue. However, this case

seemed to us to be a good one to test the constitutionality of 2511 (1) (a).

We went to trial and were successful in winning the trial at the jury level. The jury returned a guilty verdict. However, the judge dismissed the case on the ground that 2511 (1) (a) applied only to state action or, if it applied to more than state action, was unconstitutional as relates to the interception of oral communications.

We filed an appeal with the Fourth Circuit. The first issue to be overcome was the appealability issue because, of course, the dismissal had not occurred at the normal motions stage of the trial.

We lost on the appealability issue and our appeal was rejected without the merits being considered.

However, at the time of that rejection, 2 cases testing the scope of the Government's right to appeal under 18 U.S.C. 3731 were before the Supreme Court. When the Department of Justice received a partially favorable decision from the Supreme Court, we went back and petitioned for a further hearing on appealability.

That is where we are at present. The Fourth Circuit has agreed to reconsider the issue. They asked for briefs on appealability. We filed them. They have not yet asked for briefs on the merits of the case.

If I could make one comment a little bit extraneous but I think somewhat instructive as to our experience under Sections 2511 and 2512: The company that was behind the interception in the *Burroughs* case is one of the largest textile companies in the United States. It is a national company that certainly can afford to hire the best private investigators. Yet, the interception was accomplished through the representatives of the company developing an "in" with some motel employees and paying those employees, or in other ways currying the favor of the employees, so they would open the room where union organizers were planning to meet.

The representatives of the business then took their own home-made, home-constructed device made of one popsicle stick, one paper clip, and two paper matches, and using those they propped the phone up in the room where the union organizers were to meet. They then paid, or in other ways curried the favor of, the switchboard operator who opened the telephone line to the union organizers' room to the line in the next room where the textile company representatives were, so that these representatives could sit in the next room and monitor the union communications.

This—and maybe surprisingly to you after the testimony you have received in the last few days—is not atypical of the way in which investigations are

conducted, even in intrabusiness or industrial espionage investigations where certainly the money is available for the use of more sophisticated techniques. This fact leads us to conclude that, contrary to information provided by operators of countermeasure businesses, sophisticated interception devices are not readily available to persons in the private sector.

MR. HERSHMAN: Mr. Reynolds, would you give us an example of any given act of eavesdropping that would be inapplicable to the categories in 2511 (1) (b)?

MR. REYNOLDS: I have not run across one. Certainly you could hypothesize one, but we have not found a situation yet which we could not charge under Section 2511 (1) (b). We used Section 2511 (1) (a) in the *Burroughs* case because, if ever there was a case that seemed to have interstate and federal implication, it was *Burroughs*. We thought it was a good test case.

And I might mention, particularly for Professor Blakey's sake, that we are aware of his constitutional rationale for Section 2511 (1) (a), which is set forth in detail in the legislative history of Title III. That rationale is based on the fifth clause of the Fourteenth Amendment.

We have in addition sought to support the constitutionality of the section by using the rationale which flows out of a Supreme Court decision in *Perez v. U.S.*, 402 U.S. 146 (1971). We now feel that the *Perez* decision may be a better argument in upholding 2511 (1) (a). Accordingly, since we were looking not just toward use of the fifth clause in the Fourth Amendment but also to the use of the interstate commerce power, we thought the *Burroughs* case, involving a national company and a union, was a perfect case to charge under Section 2511 (1)(a).

MR. HERSHMAN: Mr. Reynolds, one portion of your opening statement, which is somewhat disappointing to me, says that your attempts at the Justice Department to refer cases of questionable federal interest to state prosecutors have met with little success. Can you give us some examples and can you tell us why that is?

MR. REYNOLDS: I don't know that I can tell you why, other than that we just encounter what appears to be disinterest, generally, at the state level.

As far as examples go, the only specific case which comes to mind immediately is one I prosecuted in Omaha, Nebraska, last summer where there was an attorney involved in what we felt to be a flagrant violation of the statutes. The court didn't feel that way and he was acquitted. We first sought to obtain an indication as to whether

the local jurisdiction was interested in pursuing the case. We particularly did that because, in this case, wiretap tapes had been introduced in a state court case and accepted into evidence by the state court judge over the objection of the opposing counsel. There had been an appeal on the issue to the Supreme Court of Nebraska. That court had cited both the federal statute, 18 U.S.C. 2515, and a parallel state statute and had ruled that the tapes were not admissible.

We waited a while to see if the local jurisdiction would prosecute. When it did not we made an inquiry as to whether they were interested: they weren't. So we handled it ourselves and I wasted a week in Omaha, Nebraska.

MR. HERSHMAN: You indicated in your statement that this is not unique, that you have experienced other difficulties.

MR. REYNOLDS: This is not unique. It is sufficiently usual that I don't have specific case names at the top of my mind. When the particular state has a statute prohibiting wiretapping or eavesdropping we frequently—particularly in domestic relations cases—ask the Assistant United States Attorneys to confer with their local counterparts. Most often they come back to us and say, "There is just no interest."

MR. HERSHMAN: In the Omaha case what was found?

MR. REYNOLDS: The jury never found anything. The prosecution was dismissed on a motion for judgement of acquittal at the end of the government's case.

MR. HERSHMAN: What was the judge's reasoning behind that?

MR. REYNOLDS: I am not sure. I requested and have examined a transcript and I am still not sure. It is pretty hard to comprehend. However, the decision appears to be based on a combination of the Fifth Circuit decision in the *Simpson* case and the willfulness standard of the statute.

And I might say the defense was rather well handled. The defense counsel argued *Simpson* to the judge off and on for three days. We were in and out of chambers arguing *Simpson*. He even argued *Simpson* to the jury over my objection. We never received a definitive ruling from the judge on the *Simpson* issue. However, the judge eventually indicated a leaning toward the Government's position on the *Simpson* issue, whereupon the defense counsel changed his tack to say in effect: "Well, Your Honor, we have argued for three days as to whether this is a violation of the wiretapping statute under *Simpson*, and maybe you are right, but it took us three days to argue it. How could my client have had any idea that what he was doing was wrong?"

The decision, unfortunately, didn't come down squarely on *Simpson*. It didn't come down squarely on willfulness. There are a lot of things interwoven in it including the right of an attorney to give advice without the risk of criminal sanctions, a principle for which a couple of very old cases were cited.

But, the real story behind that decision requires an understanding of the local situation. It was, I believe, the former head of the local bar association being prosecuted, and there was a lot of opposition and strong feeling about the case in the local bar association.

MR. HERSHMAN: Mr. Reynolds, you have been kind enough to supply the Commission with figures and statistics concerning the number of complaints received by the FBI and the number of prosecutions undertaken by the Justice Department under the Title III statute. I wonder if you know how often the civil remedies under Section 2520 have been used?

MR. REYNOLDS: I don't know. We don't have statistics on that although our belief is that it has been used very infrequently. In a number of domestic relations cases which do not appear appropriate for prosecution under the existing felony statutes, for example those where no private detective or other professional is involved, we have Assistant United States Attorneys watch to see if any action is initiated under Section 2520. The answer almost uniformly is no. Also, if you will look at the annotations under 2520, in U.S. Code Annotated, you will find that it is a statute almost without annotation.

MR. HERSHMAN: Does it appear to you, Mr. Reynolds, that the individuals involved as victims of electronic surveillance are hesitant for particular reasons to file for civil remedies?

MR. REYNOLDS: In domestic relations cases I think the answer is that there is a specific reason. We find that the victims of domestic relations electronic surveillance are quite frequently very hesitant government witnesses. They don't want to be involved. In some cases we have received an affirmative indication that they are afraid that facts about their personal life would come out at trial. I surmise that this is normally the reason for their reluctance to cooperate with the government. I am sure that the same reluctance would be involved in other types of electronic surveillance cases. Further, the same fears would serve to discourage victims from bringing a civil suit under 2520.

Let me mention one other thing, Mr. Hershman, on this. Our experience in the domestic relations area is that there is very often an attorney somewhere in the periphery of domestic relations electronic surveillance violation. It is not easy, par-

ticularly in smaller towns, to get one attorney to institute a civil action which may cast doubt on the ethics of another attorney in town. We have seen specific instances of this. In the case that I mentioned in Omaha, Nebraska, where we prosecuted an attorney, one of the victims was adamant about bringing a civil suit. He finally was successful, after going from one attorney to another, in finding one who would institute a civil suit. However, he never found one, the last I heard of the case, who would name the attorney as a defendant in the civil suit.

Did I cut you off on statistics?

MR. HERSHMAN: Well, you raised another point and I am glad you did.

How many cases have been brought against attorneys for complicity in illegal wiretapping?

MR. REYNOLDS: The figure is, to the best of my knowledge, six cases.

MR. HERSHMAN: Since when?

MR. REYNOLDS: Since 1968 when the statute was passed.

MR. HERSHMAN: That is nationwide?

MR. REYNOLDS: That is nationwide. The reason that the figure may appear low is that we try to make sure we have a strong case before we proceed against an attorney. We often encounter unsympathetic judges in the prosecution of a local attorney. The United States Attorney's offices will cooperate with us but normally they don't want to supply an Assistant United States Attorney, particularly in smaller districts, to try the case. This necessitates our sending an attorney from Washington into an environment he is not acquainted with and where there may be some hostility toward him. Therefore we try to make sure that we've got our case together so that nobody can say that federal officials from Washington are coming in on a witch hunt. Even having applied that standard, we have lost the first five prosecutions we brought against attorneys. Four of those five cases never got to a jury.

MR. HERSHMAN: When you speak of sending a Washington attorney, I assume you would enter the case or one of the attorneys assigned to your section?

MR. REYNOLDS: That is right.

MR. HERSHMAN: How many attorneys are assigned to your section?

MR. REYNOLDS: Myself and three other people.

MR. HERSHMAN: So there are four attorneys concerned with prosecutions of violations under Title III; is that correct?

MR. REYNOLDS: That is right: Sections 2511, 2512 of Title 18 and 47 U.S. Code Section 605.

MR. HERSHMAN: Do you have any other responsibilities in your section?

MR. REYNOLDS: Yes, we have responsibilities for assaults on federal officers and murder of federal officers, assault and murder of foreign officials, counterfeiting, postal offenses and theft of government property.

Let me say, however, that it is not four attorneys in the Criminal Division who alone carry on the crusade in enforcing Title III. Obviously, we don't investigate cases; the FBI investigates cases and their resources are available to us and similarly the bulk of the prosecutions are handled by Assistant United States Attorneys who generally cooperate very well with us. We normally have a very good partnership. So it is not just four people in Washington that are handling the prosecution of these cases.

MR. HERSHMAN: Mr. Reynolds, I would like to discuss the Justice Department's policy towards enforcement of illegal wiretapping in domestic situations. You note in your opening statement that the legislative history of Title III explains that it is particularly applicable to electronic surveillance conducted in domestic situations and industrial espionage cases.

If we don't enforce the cases against marital espionage where no professional interceptor is involved, that leaves very few other cases left, isn't that right?

MR. REYNOLDS: I think that is a good point and I think it points up a problem with Section 2511 that needs to be examined. A very high percentage—our figures indicate not less than 75 percent of the interception of communications violations are domestic relations in nature and a significant percentage of those don't involve a professional. So, it is hard to curb electronic surveillance without proceeding on those cases. However, we just don't have in the existing felony statute with a high standard of criminal intent what we normally feel is the right tool for going after a husband for wiretapping the wife or the wife the husband, or a father wiretapping his 19-year-old daughter.

If you want to see a hostile court, imagine a prosecution of a father who is eavesdropping on his 19-year-old daughter who he is afraid has a drug habit. Such a case is very difficult where you attempt to prosecute using a felony statute and the standard of willfulness embodied in *U.S. v. Murdock* 290 U.S. 389 (1933).

One point of interest about the non-professional interception of cases in domestic relations cases: We get a significant number of cases where a telephone company repairman discovers and removes the interception device from the telephone. He then notifies the FBI, and the FBI goes out and talks to whomever they find in the

home. Maybe they talk to the wife who is the apparent victim of the intercept, and she says, "I am sure it is my husband. We are involved in a domestic relations dispute. I am sure he did it." The next step is to interview the husband. In a significant number of cases, when the husband is interviewed following a rights advisement, he says, "Yes, I did it. I didn't know there was anything wrong with tapping your own phone." Either this husband has been awfully clever—which I doubt—or he didn't know his action constituted an offense. Using the medium of felony prosecution and applying *Murdock*, you have a virtually impossible situation as far as prosecuting that case.

MR. HERSHMAN: Is it difficult to prove malicious intent where a wife is trying to obtain a better settlement in a divorce proceeding against her husband?

MR. REYNOLDS: I am not sure I understand the thrust of the question.

MR. HERSHMAN: The thrust is this: Many illegal wiretaps in domestic situations arise out of a desire of one of the spouses to obtain a better settlement in a divorce situation. Is that not malicious intent?

MR. REYNOLDS: That may be a malicious intent in the common use of the word, but whether that is sufficiently willful conduct under the *Murdock* standard is another question.

Murdock sets forth the requirement of malicious intent and then the court proceeds to cite approvingly a couple of cases which indicate that the individual must have a careless disregard for whether he is violating the law, and must have no ground for believing that his act is legal. When you interview someone and they say, "Yes, I did it; I didn't know it was wrong," you have a tough row to hoe under that standard.

MR. HERSHMAN: Mr. Reynolds, for the past few days we have been taking testimony from individuals who are familiar with the statute, with 2511 and 2512. They deal with them very frequently. They are the people involved in debugging offices and phones. They are the individuals involved in the manufacture, sale and advertisement of electronic surveillance equipment.

It seems to me that the testimony and the evidence presented indicates that there is a proliferation of illegal devices for sale on the market today.

I would like to know what steps the Justice Department or the FBI are taking in order to determine what equipment is illegal, and who is advertising and selling it.

MR. REYNOLDS: The basic foundation of our enforcement of Section 2512 is through the

response to complaints. If a complaint is made—and usually the complaint comes in from a competing manufacturer—we investigate it. The complaints are not allowed to go without investigation.

To follow up on this complaint-oriented system of enforcement, we occasionally go forward with an affirmative approach, picking a particular area and trying to determine on our own without a complaint whether stores are offering for sale devices that would violate 2512. However, the normal foundation of the policy is to respond to complaints.

MR. HERSHMAN: I would like to know how occasionally it is. How many affirmative action programs occur?

MR. REYNOLDS: It has been quite occasional. The last such program was last summer.

MR. HERSHMAN: Before that, how many?

MR. REYNOLDS: You are going back into my pre-Justice Department time. I really can't tell you exactly, although I am aware, from one of my predecessors, that it has been done in the past.

MR. HERSHMAN: I wonder, Mr. Reynolds, if you would submit a letter to us at a later date specifying just how often these affirmative programs have taken place and in what form they have taken place—where and when, and what results were gained from them.

MR. REYNOLDS: You are being more formal than our programs have been. The programs usually consist of a memorandum or a call to the appropriate personnel at the FBI, requesting that they make checks in certain specified cities. Then the results come back in the form of our normal flow of FBI reports.

MR. HERSHMAN: Mr. Reynolds, I might suggest that the National Wiretap Commission, with its very limited resources, has managed to uncover numerous advertising violations simply by reading through magazines.

I have included in our hand-out to the Commissioners advertisements of electronic surveillance equipment that I obtained simply by answering advertisements in magazines such as *Argosy*, *Popular Electronics* and *Popular Mechanics*. How difficult would it be for the FBI or the Justice Department to sit down and read a magazine?

MR. REYNOLDS: That has not been a part of our program in recent years. It is my understanding it was a part of the program at the initial stages of our enforcement of the statute when we had to clear up the rash of advertisements that were appearing in magazines. But as those advertisements appeared to subside, the program of reading the magazines was discontinued. To the extent that it is necessary to reinstitute that, it can be reinstituted

on some basis. But, right now there is no program of reading magazines. About the only thing we pick up is something we would normally read ourselves. For example, we picked up one violation in an advertisement in the *ABA Journal*.

CHAIRMAN ERICKSON: We heard of one in *Playboy* yesterday that a witness read on his way from California. And that was made part of the record and it was a blatant violation of the statute.

MR. HERSHMAN: The security director of Hewlett-Packard was here and said he had received through the mail unsolicited, blatantly illegal advertising material. I might say we have secured the same thing from various private investigative firms. They do indicate that these are turned over to the Federal government, the United States Attorney's offices in the respective jurisdictions.

But frankly, the number of cases brought since 1968 just don't reflect that many prosecutions under Section 2512.

Mr. Reynolds, do your affirmative action programs, when they occur, go further than 2512? Do they go into areas of 2511 to try to determine what individuals, what private investigators have available or are offering available electronic surveillance services to the public?

MR. REYNOLDS: No, we have not done that.

MR. HERSHMAN: The Commission conducted a study where we contacted 115 private investigators in seven cities in the United States. A good number of these—I believe 42—indicated to us that they would perform for us an illegal wiretap or bugging.

I would like to know why you can't do the same thing.

MR. REYNOLDS: Prior to this hearing, you provided me an explanation as to how you conducted your study.

Certainly there are some steps we can take to ferret out this type of illegal activity, but what you did, I would say, would run us afoul of entrapment.

MR. HERSHMAN: I would turn the answer to that over to Professor Blakey or Chairman Erickson.

PROFESSOR BLAKEY: Are you familiar with *Russell*?

MR. REYNOLDS: Yes, I am, sir.

PROFESSOR BLAKEY: Would you analyze Mr. Hershman's conduct under *Russell* and explain to me why that is entrapment?

MR. REYNOLDS: Where you are engaging in random calling, you are asking someone to commit an offense without any knowledge of predisposition on their part to commit the offense—

PROFESSOR BLAKEY: Suppose they had taken ads from the yellow pages that said "Debugging"

and called up people that used the word "Debugging," which is, as you know, frankly, a code word in the community and simply asked if they were willing to engage in electronic surveillance. Surely it is not your testimony that that constitutes entrapment.

MR. REYNOLDS: I would have to make a judgment on the specific situation, considering what was said on the part of Mr. Hershman, or whoever made the call.

PROFESSOR BLAKEY: This happens to me in class all the time, with students who understand "entrapment" to mean "tricky." But, if you carefully analyze the case it says—the Supreme Court in *Russell* went about as far as it could go—that providing an essential service to the other side and affirmatively moving against him was held not to constitute entrapment.

And frankly it seems to me if the Department is unwilling to make some random calls and offer a person an occasion to commit an offense—not importuning but offering an occasion to do it—this statute will not be enforced.

If you are operating only on the basis of complaints in the domestic relations area, and the only time you prosecute in those cases is for third-party intercepts and you don't go against the people in the two-party intercepts, you are not enforcing the statute. You are not going to—the chances of stumbling into a tap in operation are small. You won't find it by street patrol. You must have an affirmative action program.

If the Department has manpower problems, that is understandable. If they have higher priorities, that is understandable. But to fail to take the only affirmative action available to you in this program is allowing these people to continue their conduct largely without interference—and, frankly, they are continuing it.

There were discussions on the staff level when they planned their actions whether that would constitute entrapment, and there was a clear feeling that under existing case law it didn't. And I am very disturbed you use that kind of simple guise to hide your failure to act. It is simply not entrapment. It is a failure—

MR. REYNOLDS: Let me say the decision of the Department of Justice not to use more affirmative action in this area has been based primarily on a question of resources. It is a question of how much you allocate in one area versus another. We are not dealing with an unlimited amount of resources. Normally, when you put into one area you take away from another area. But certainly we are open to ideas on affirmative action.

PROFESSOR BLAKEY: That is perfectly understandable. Nobody could argue that every Bureau office in the country ought to have the same kind of affirmative action that, say, DEA has against narcotics. But to find no affirmative action program by any Bureau office in the country, no affirmative action program by any United States Attorney's office or no affirmative action program out of a small unit in Justice since 1968 is not just to say that you haven't resource power; it is to say as a matter of policy you have decided not to use affirmative action at all.

If you only did it once every six months and did it in odd-numbered cities, you would put such a scare into the private detective people that they wouldn't do it any more or they would substantially curtail their activities.

MR. HERSHMAN: I think, Professor Blakey, that there are United States Attorneys' offices in the country—one in particular—that have affirmative action programs. The one I am thinking of is the United States Attorney's office in the Southern District of New York. They have an affirmative action program which is being run by their independent criminal investigators, and to date I think it has been highly successful. Certainly it has led very recently to the arrest in New York of not only a private investigator but a manufacturer of electronic surveillance equipment.

I would like to say, Mr. Reynolds, it is not difficult to initiate an affirmative action program. We had appearing before us yesterday a number of people involved in countermeasure programs who have found, over the years, thousands of illegal wiretaps. They almost never notify law enforcement, and have not been contacted by the FBI. If the FBI perhaps took time out to contact some of your debugging people and asked them to cooperate on illegal finds, I think they just might. I get the indication they would.

MR. REYNOLDS: These people have never turned over any evidence on devices that they have taken off?

MR. HERSHMAN: Very, very seldom. They inform their client. The gentleman from Pinkerton advises the client very strongly to call the FBI and the United States Attorney's office but after that he walks out the door. And some of the others don't even bother to inform them to call the police.

Now, I think my interpretation of their feelings is that they would be willing, perhaps, to cooperate to a greater degree with law enforcement if the opportunity existed.

I also wonder about the discrepancy in the finds of illegal wiretaps and eavesdropping devices by the telephone company and the reporting of those finds

to the Federal Bureau of Investigation. I can't understand why that exists.

Is there no liaison between the FBI and some of the subsidiaries of Bell Telephone?

MR. REYNOLDS: I was unaware that such a discrepancy existed. As soon as we discovered its existence, we took action to close that gap. It had previously been our understanding that the FBI received reports of all devices taken off of telephones.

MR. HERSHMAN: But obviously that did not happen.

MR. REYNOLDS: Apparently, from your statistics that wasn't happening.

MR. HERSHMAN: Mr. Reynolds, in your opening statement on page 6, you state that:

"On several occasions United States District Court judges have been openly defiant of Government efforts to prosecute 2511 violations."

I wonder if you could give us some examples of that, please.

MR. REYNOLDS: I can give you examples by general substance. I would prefer to do that, rather than list case names. In one situation involving the prosecution of an attorney, we received a great deal of pressure from a federal district court judge to acquiesce to a guilty plea to an inapplicable misdemeanor. In the particular situation we weren't terribly aggrieved by the principle of allowing a plea to a misdemeanor but there didn't appear to be an applicable one. The Assistant United States Attorney received a tremendous amount of pressure in that case, to the point where it was felt that we would have very little chance of success in a prosecution.

There was a case approximately a year ago in North Carolina where there was active intervention by the federal district court judge with the United States Attorney's office, in effect, pleading that we were going to put the private detective out of business if we prosecuted him, because a felony conviction would cause him to lose his license. The judge pointed out to us that the defendant employed approximately 30 people and there was a strong suggestion that it would be best to drop the case or at least reach some settlement. Eventually, we acquiesced to a *nolo contendere* plea.

To give an example of a reported case, the *Christman* case out of San Francisco appears to represent a certain amount of judicial dislike for our wiretapping prosecution.

MR. HERSHMAN: I wonder if we might not hold off on that case until we get to the portion of your testimony concerning service observing.

Mr. Reynolds, of course we all understand that you don't set Justice Department policy. I would

like to get your personal views as to what priority is set in the Justice Department on illegal wiretapping and electronic surveillance.

MR. REYNOLDS: Let me say that while I do not, of course, have final approval power over the Department's policy of enforcement of the criminal sanctions against wiretapping and eavesdropping, I do have an input in that policy and a responsibility for proposing changes in policy. The priority, as indicated earlier, is one of attempting to focus on the professional; the highest emphasis is placed on the professional interceptor and those who engage in or procure such activity as part of their business. Accordingly, emphasis is placed on industrial espionage and law enforcement violations; particularly law enforcement.

MR. HERSHMAN: Mr. Reynolds, is it given the same priority as affirmative action programs concerning the interstate theft of automobiles?

MR. REYNOLDS: You are taking me into an area where I am really not familiar with the Justice Department program.

MR. HERSHMAN: Do you feel, Mr. Reynolds, that you could accomplish more in identifying and prosecuting cases of illegal wiretapping and the illegal sale and advertisement of wiretap equipment if, in fact, you were given the aid of more attorneys in your section?

MR. REYNOLDS: I think anyone who tries to do his job conscientiously feels that he could use more people. But down the hall from me is a unit about the same size as mine that works on bank robbery and kidnapping. I know that they are extremely busy and feel they need more people. Again, there exists a relatively constant pool of personnel from which to draw. It is necessary to determine what is the proper allocation of personnel to the various problems. Frankly, I am not the one in the Department who sits in the best position to make those judgments. I see my areas; I know the needs of my areas. But when you mention cargo theft or interstate transportation of stolen property you are into areas where I am not familiar with their enforcement policies or their problems.

MR. HERSHMAN: Do you feel frustrated in your area because you can't do more?

MR. REYNOLDS: I think I am more frustrated by some of the problems we have run into with the statute than by a lack of personnel. For example, the fact that the only sanction available under the statute is a felony prosecution with a *Murdock* standard of criminal intent is a cause of frustration in that we lack flexibility in responding to the varying types of violations. I think that is more of a frustration now than a lack of personnel. But certainly there are more things we would do and things we would do better if we had more personnel.

MR. HERSHMAN: Mr. Reynolds, you speak of the need for an alternative to felony prosecution. We took testimony on Monday from an Assistant United States Attorney in the Southern District of New York who testified that he successfully prosecuted, under Civil Rights statutes, misdemeanor violations.

MR. REYNOLDS: Right. I would say you could use 18 U.S.C. 242, deprivation of rights under color of law, as a misdemeanor offense, but my reading of that statute would make it applicable only to law enforcement violations. If there is ever a type of case where the felony prosecution is generally appropriate, it is the law enforcement violation. I would be interested to see any theory that would say we could use that Civil Rights statute for private, non-law enforcement violations of the wiretapping statute. But, I am unaware of any theory in that regard.

MR. HERSHMAN: I would like to go a little bit more in depth into the *Simpson v. Simpson* case, Mr. Reynolds.

In talking with you before the hearings I understand that you disagree somewhat with the finding of the court. Is that correct?

MR. REYNOLDS: Well, the disagreement is best summarized by saying that I think the decision is wrong. It is contrary to the legislative history of the statute.

But, in one regard, the court deserves credit. It decided the case on the legislative history and in so doing allowed us to scrutinize the underpinnings of its decision by setting out in footnotes exactly what legislative history it found. So, we can, in a sense, grade the court. What did they find; what didn't they find? They did a lot of digging. They went back into a lot of legislative history that is pretty obscure. However, unfortunately they missed some of the more obvious legislative history, including portions of the Senate Report 1097, 90th Congress, 2d Session (1968), which accompanied the legislation out of the Senate Judiciary Committee and also some of the key hearings on the Right of Privacy Act of 1967.

I believe the court missed the whole rationale of Professor Blakey's testimony concerning why his proposed bill should be adopted as opposed to the Justice Department bill.

The court also missed the statement by Senators Dirksen, Hruska, Scott, and Thurmond to the effect that the statute is designed particularly for domestic relations and industrial espionage and surveillance. The court also missed the statements concerning the blanket nature of the prohibitions in Section 2511.

PROFESSOR BLAKEY: Why did they go to the legislative history at all? If the statute is clear, you don't need to.

MR. REYNOLDS: I don't think they needed to. However, we feel that we can counter the reasoning of *Simpson* at either level: the wording of the statute or its legislative history. If you go to the words of the statute, they provide clear coverage to interspousal electronic surveillance. The words of the statute are clear and that should be enough. But the court appeared to have an overwhelming desire not to rely solely on the words of the statute. The court seemed confounded by the fact an ex-wife could sue her husband in a tort action for wiretapping.

The court seemed surprised that Congress would enact a statute that would make it a criminal violation for one spouse to wiretap another spouse within the marital home. The court mentioned, with some seeming concern, that if they held there was a cause of action under Section 2520, that would also mean that the husband was guilty of a federal criminal offense. That appeared to bother them; they didn't want to reach that result so they looked at the legislative history.

However, we certainly would make the argument that on its face the statute reaches the conduct of Mr. Simpson in tapping Mrs. Simpson. In fact, the court even agreed with that. We can counter the decision on that level, and we can counter it well on the legislative history level.

The problem with *Simpson* is not so much in meeting it head-on, because we feel we can prevail there. The problem with *Simpson* is its derivative effect on the issue of willfulness. The argument we are now having to confront is, if the Fifth Circuit could have been so uncertain as to whether intra-family wiretapping is a violation of the law, how can you expect my client to have had any idea he was violating the law? That is where we are getting hurt right now. We are looking for a case that is an appropriate vehicle to challenge the *Simpson* ruling. We had three prosecutions in the last six months or so of one spouse for wiretapping the other. They fit right into the *Simpson* situation. We were looking for a test but the defense didn't raise *Simpson*.

MR. HERSHMAN: Did those cases have a professional interceptor involved?

MR. REYNOLDS: No.

MR. HERSHMAN: Who decides which cases are prosecuted when one spouse eavesdrops on another?

MR. REYNOLDS: It is a somewhat mutual decision; an amorphous arrangement between the cognizant United States Attorney's office and the Criminal Division. The first crack at the decision

belongs to the United States Attorney's office. If they decide to go forward on a case, rarely, if ever, will we countermand that decision. I don't know if there was ever a case when we pulled the United States Attorney's office back from prosecution. Our normal procedure is to review the cases they don't prosecute and if we feel that such a case clearly needs to be prosecuted we discuss the matter with the U.S. Attorney's office in an attempt to reach some accommodation.

MR. HERSHMAN: Mr. Reynolds, is it true that the ruling in *Simpson v. Simpson* has led to an increase in private investigators being involved in marital eavesdropping?

MR. REYNOLDS: My initial reaction is no, but I really don't have any figures or solid basis from which to reach a valid judgment on that point. I know that *Simpson* has been misconstrued in the press. We received a few inquiries enclosing news articles from around the country which indicated, at the time the Supreme Court refused to grant certiorari on the case, that the Supreme Court had upheld the right of one spouse to wiretap the other spouse. We answered those and attempted to correct that misunderstanding, but to the extent there is publicity like that, certainly I think there is a risk that a private detective who had restrained himself before might begin to engage in electronic surveillance in marital cases.

MR. HERSHMAN: Let me ask, Mr. Reynolds: To what extent must a private investigator intercede in a case before you consider it professional involvement? What if he just supplied the equipment?

MR. REYNOLDS: We consider such supplying of equipment to be an involvement, if the private investigator knew what he was supplying the equipment for. Most of the violations of 2511 we are seeing involve the use of non-proscribed devices. Obviously, if the private investigator supplies a proscribed device under 2512, we would proceed from that angle. But, if he supplies a device not proscribed under Section 2512, we would have to obtain evidence that he knew what use was going to be made of the device. If we can develop such evidence, then we consider the private investigator to be part of the case and he would become a primary target.

MR. HERSHMAN: What if he tells his client where to buy the device and how to install it?

MR. REYNOLDS: You are getting into an aiding and abetting, and—

MR. HERSHMAN: I want to know at what point you consider the involvement a professional interceptor.

MR. REYNOLDS: If we can establish a prosecutable case at any level against a professional, then we consider the professional to have been in the case.

MR. HERSHMAN: What if an attorney recommends that a client see a private investigator who he knows will engage in illegal electronic surveillance?

MR. REYNOLDS: That situation is one step removed, and it is starting to get difficult as far as prosecution. But again, we would take a very close look at that situation. Attorneys certainly have to be a primary target of our prosecutive policy and anytime there is any indication of attorney involvement, we make sure that an investigation is conducted to the fullest to determine what that involvement is. But, let me point out there are some difficult problems of proof when we try to establish what an attorney knew about a private detective's action. We are generally not able to obtain the testimony from either the attorney or the private investigator. We are obviously not going to immunize the attorney, and it is unusual to get anything out of the private investigator.

MR. HERSHMAN: Turning for a moment to service observing, you note that it is difficult to justify the activity that is sanctioned by Section 2510 (a).

Would you explain why it is difficult to justify that?

MR. REYNOLDS: That wasn't exactly what I was intending to get across.

MR. HERSHMAN: That is what you said, though.

MR. REYNOLDS: It is not that it is difficult to justify all service observing activity but it is difficult to justify the scope of the exception contained in Section 2510 (5). In other words, it appears to allow intercepts that would be difficult to justify. But I don't mean to criticize the whole service-observing concept.

I think there might be some validity to the existence of a service-observing exception in the statute. But 2510 (5), the way it is written now, as I read it and interpret it, would not require notice to the person whose conversations are being overheard.

This is the point we feel is onerous about 2510 (5).

There are a couple of other points about Section 2510 (5) which deserve comment. Again as I read 2510 (5), it simply exempts service observing equipment from the definition of a "device." It contains no standard to govern who can possess such equipment and to delineate its limits of permissible use, and I am not sure that that is wise. Also it appears to establish a monopoly in commu-

nications common carriers in service observing equipment, which again appears unwise.

Let me say that whole statute, Section 2510 (5), is a very difficult provision to construe and a very difficult provision to trace through the legislative history. The statutory interpretation I have provided is based on our best judgment on what the legislative history is and what it allows.

MR. HERSHMAN: I am not quite sure I understand what portions of 2510 (5) you are uncomfortable with.

MR. REYNOLDS: I am uncomfortable with the fact that it appears to me that if the communications common carrier furnishes service observing equipment to a business, that service observing equipment can be used to intercept the conversations of employees without notification to the employees. Let me say here that I understand that as part of the telephone tariffs, there is generally imposed upon the businesses that receive this service observing equipment an obligation to notify their employees. However, I think consideration should be given to requiring such notification as part of the statute.

MR. HERSHMAN: I would like to turn at this time to the Macy's case, which you mentioned earlier. Would you explain to the Commission, please, the circumstances surrounding that case?

MR. REYNOLDS: It is a difficult case to analyze because the decision by the Federal District Court Judge has interwoven into it a number of different theories. But the facts behind the case *U.S. v. Christman*, 375 F. Supp. 1354 (N.D. Cal, 1974) are that the security chief of the department store felt he had a problem in his shoe department. He was suspicious of narcotics use by the employees, prostitution, misuse of the telephone, and theft of property from his shoe department.

CHAIRMAN ERICKSON: All that in a shoe department?

[Laughter.]

MR. REYNOLDS: It must have been some shoe department—all this in one department. At least that is what the decision tells us. So his way of investigating the situation was to have an extension telephone installed onto the extension telephone line of the shoe department.

CHAIRMAN ERICKSON: Was this the organized crime shoe department?

[Laughter.]

MR. REYNOLDS: It could have been. But, it might have been the local vice shoe department—at least if all the suspicions were founded. At any rate, he hooked this extension telephone onto the extension telephone wire of the shoe department and proceeded to use his extension telephone to record

the conversations of employees in the shoe department. The security officer, Mr. Christman, was subsequently prosecuted by the Department of Justice for the interception of wire communications. And the Federal District Court Judge dismissed the case, holding that the statute did not apply to the acts of Mr. Christman. The judge used several different legal theories as the basis of his dismissal.

First, he concluded that the extension telephone is excepted from the definition of a device under 2510 (5), and therefore use of it does not constitute an interception of communications. To the extent that Section 2510 (5) excludes extension telephones, the exclusion only applies to those "installed in the normal course of business." Somehow the judge concluded without explanation, that in this situation this extension phone had been installed in the normal course of business. Second, he ruled that in his judgment there was no expectation of privacy on the part of the people using the telephone. The issue of expectation of privacy appears irrelevant as the standard in the statute for wire communications is one of consent as opposed to expectation of privacy.

Finally, the third area that he struck upon was that under 2511 (1) (a) (i), the communication common carrier has the right to do necessary and reasonable monitoring for protection of property. The judge construed the department store to be a private carrier of communications, and ruled that they were simply trying to protect their property. Thus, he concluded that they had a right to intercept under 2511 (2) (a) (1). To us, this conclusion seems to defy the definition of "communications common carrier" as set forth in 2510. So, those were the three basic points raised in support of the decision, all of which we disagree with.

It is interesting to compare the wording at the end of his decision with the closing portion of *Simpson*. In *Simpson* the court said, "We are limiting this decision strictly to the facts," and the judge in *Christman* said that, too: "We are limiting this to the facts."

I think to fully understand and get the flavor of the *Christman* decision, you have to look at the portion of the transcript that leads up to the dismissal of the case. And, if I could read just about one page of transcript, I think it is enlightening. This is the judge who is speaking first:

"As I pointed out earlier, the statute did not seem to be designed to reach this kind of a situation."

Skipping down about five lines: "Nor can I say, as a matter of common justice, that I am upset this must be the result. It seems to me that it is inappropriate for the United States Attorney's office to

cooperate so handsomely with persons who seemingly are using it for private purposes."

"It" appears to be phones.

Assistant U.S. Attorney: "I don't think that has been established, your Honor."

The Court: "It seems plain here if there were any violation that it might be a violation of state law. I must assume that state authorities were first approached on the more clearly applicable statute, and I must presume they refused to participate."

Assistant U.S. Attorney: "They were not interested."

The Court: "I can understand that they would not be. I am surprised that the United States Attorney was."

Assistant U.S. Attorney: "I think those comments are unfair, Your Honor, to our office."

The Court: "There may be reasons that I am not aware of that required this action to be brought. I have always thought the United States Attorneys had a certain amount of discretion in determining whether a case properly should be presented."

Skipping down about three lines: "I am not convinced that the defendant is a felon or should be declared so."

CHAIRMAN ERICKSON: What judge was that? And where was the case?

MR. REYNOLDS: The case was in the Federal District Court in San Francisco; Schnacke was the judge.

I think this portion of the transcript points up interesting foundation behind that decision. I submit that decision is a rather scatter-gun type approach to the law. It reminds me of the old adage, "if you don't have one good argument to make, you use a lot of lesser arguments." I do not think that any one of the areas that the judge struck upon really has any merit to it at all, and I would further say that the judge's reaction to the facts of this case is not atypical of judicial reactions that we have experienced. What is worrisome is that if judges react this way to some of our prosecutions, one wonders sometimes what occurs in the jury room.

MR. HERSHMAN: Mr. Reynolds, for the purpose of your enforcement program, have you been able to make any rule of thumb determination concerning the language "in the ordinary course of its business" with reference to subscribers?

MR. REYNOLDS: Are you referring to 2510 (5) (a) still?

MR. HERSHMAN: That is correct, (5) (a).

MR. REYNOLDS: We have recently engaged in much work on the legislative history of that section 2510 (5) (a) and our interpretation of that provision has changed somewhat. It used to be felt that 2510 (5) (a) was primarily an exclusion of exten-

sion telephones from the category of intercepting devices. Under that interpretation the intention of 2510 (5) (a) was to avoid a massive number of picayune extension telephone violations. No matter what use was made of an extension telephone installed in the normal course of business, there would not be a violation of the law absent the use of another device, such as a tape recorder, to record what was being received over the extension telephone.

We used that argument in *U.S. v. Harpel*, 493 F. 2d 346 (CA10, 1974), and the court didn't embrace our argument. The court indicated a tape recorder could not be deemed the intercepting device since the extension phone was the device that provided access to the communications. The tape recorder simply preserved what has already been intercepted.

Despite rejecting our argument, the court gave us what was, in finality, a favorable decision. They homed in on this requirement in the exception—2510 (5) (a)—that the use of telephone equipment be in the regular course of activities. They concluded that it can't be the regular course of activities to use an extension telephone to snoop.

After that decision, we began going back into the legislative history to determine whether the position we had been taking or the *Harpel* position was right, and I must say it is difficult to trace the language of Section 2510 (5) (a). The four bills that were, in substance, the predecessors to the existing statutes all possessed a 2510 (5) (a) type provision which applied either to hearing aids or to extension telephones—one or the other, or both. It appears to us that the language we now have in 2510 (5) (a) is traceable to testimony of FCC Commissioner Lovinger and to AT&T operations official Kurtz. They both testified before a Congressional subcommittee on the proposed Right of Privacy Act of 1967 where they raised the issue of service observing. Their testimony brought out the fact that communication common carriers had a large market in service observing equipment. Sometime after that testimony, 2510 (5) (a) was changed and we had the addition of the words "being used in the ordinary course of business."

While it is a little difficult to construe that language, if you interpret it the way the *Harpel* court did, it appears that Congress torted with a telephone extension exception that eventually got thrown out in favor of a service observing exception.

To summarize, under the *Harpel* decision, "ordinary course of business" would mean the normal use of the instrument for what it is designed to be used for. It wouldn't include picking up an extension telephone to spy on another party.

MR. HERSHMAN: Turning for a moment, Mr. Reynolds, to Section 2512, how does the Justice Department determine when a device is preliminarily useful for the surreptitious interception of wire and oral communications?

MR. REYNOLDS: I think we have to go back to the definition contained in Senate Report 1097 for the best statement as to what is primarily useful for the surreptitious interception of communications. It indicates that to be prohibited the device would have to possess attributes which give predominance to the surreptitious character of its use. That is the basic definition with which we start and we then rely heavily on the examples set forth in Senate Report 1097 as to what constitutes an illegal device. These would include an infinity transmitter, a spike mike, and a number of disguised listening devices, such as cuff link microphones and tie clasp microphones.

So our judgment as to what devices are "primarily useful" is based on, number one, the definition and number two, on the examples. From those two factors we conclude that basically 2512 is designed to prohibit (1) disguised listening devices, and (2) devices that are designed to intercept communications occurring elsewhere than the location of the interceptor.

MR. HERSHMAN: Mr. Reynolds, can you think of any purpose of using a cuff link or tie clasp microphone other than to intercept one-party consent conversations?

MR. REYNOLDS: You can conjure up a strange situation, but the normal use is for a one-party consent interception.

MR. HERSHMAN: And do you see any conflict between the provisions of 2511, which allow for one-party consent and 2512 which prohibits devices which can be used for one-party consent monitoring?

MR. REYNOLDS: No, I don't at all. However, some courts have. The first such case was the *United States v. James A. Six* (D.C.N.D. Indiana, 1970). According to the court, a person is not in violation of 2512 unless he not only willfully possessed the device, but intended to use it in violation of 2511. We have argued that this is the wrong interpretation. We had a similar type decision rendered in the case of *United States v. Bast*, 348 F. Supp 1202 (D.D.C., 1972); vacated 495 F. 2d 138 (C.A.D.C., 1974). We appealed to the U.S. Court of Appeals for the District of Columbia Circuit and received a favorable decision in what I think is a very well reasoned, clear opinion. It indicates you don't read the exceptions of 2511 into 2512.

MR. HERSHMAN: Mr. Reynolds, on Wednesday of this week we had a demonstration and display of various types of electronic surveillance devices.

One of the devices that we saw was an aspirin-sized transmitter. The transmitter contained a built-in microphone and battery source—no larger than an aspirin.

On its face, would that device, which is not concealed or designed to be anything else be prohibited under 2512?

MR. REYNOLDS: Not per se; at least not under the facts you have given so far.

MR. HERSHMAN: Isn't it obvious that a device of that nature has much more dangerous potential than a cuff link microphone or a tie clasp microphone?

MR. REYNOLDS: It may have dangerous potential. However, there are two problems. One is that the legislative history of Senate Report 1097, indicates that size alone is not the criterion in determining whether the device is "primarily useful."

The second problem is that you have a number of normal and legitimate nonsurreptitious uses for small transmitters. For example, the television industry makes fairly great use of the parabolic mike. So you have a couple of problems in trying to bring the device that you are talking about within the definition of "primarily useful" under 2512.

MR. HERSHMAN: So that under the current statute, regardless of how small a device becomes, it is not necessarily prohibited?

MR. REYNOLDS: Not necessarily.

MR. HERSHMAN: I am talking about a transmitter.

MR. REYNOLDS: The answer would be that in our view it is not necessarily prohibited; right.

MR. HERSHMAN: But yet the use of some of these devices could provide a greater danger toward invasion of privacy than some of the devices which were originally listed in the legislative history of Title III; is that correct?

MR. REYNOLDS: I think that is certainly possible and it relates to a fact I mentioned earlier about the violations that come to our attention under Section 2511. Most of them don't make use of a device which violates 2512. The oral intercept violations of 2511 we see are almost always done with a small FM transmitter—nothing as sophisticated as the aspirin-sized transmitter that you are talking about. Rather a cigarette pack-sized FM transmitter is generally used.

MR. HERSHMAN: Your statement, sir, says that it appears that the devices proscribed by the statute are of two basic types: One, disguised listening devices—which is very clear—and, two, devices designed to intercept communications occurring elsewhere than the location of the interceptor.

Would that not, in fact, then, say that all body transmitters would be prohibited by 2512, since a

body transmitter is designed for interception at a location other than the place of reception?

MR. REYNOLDS: I am not sure I follow you. Body transmitters—

MR. HERSHMAN: You wrote here "devices designed to intercept communications occurring elsewhere than the location of the intercept."

MR. REYNOLDS: That was with particular reference to cover an infinity transmitter or a spike mike.

MR. HERSHMAN: This also covers every body transmitter on the market today that is used for officer safety.

MR. REYNOLDS: I'm not sure I see that.

MR. HERSHMAN: A body transmitter works on the principle that the intercepted conversation is transmitted to a remote listening point.

MR. REYNOLDS: That may be, but the point of interception is the place where the transmitter is located and where the person providing one-party consent is located.

I don't mean for anyone to get hung up in these two categories that we have created. We didn't create them as regulations and haven't promulgated them as such. To the extent that you find our two categories more difficult that the application of the words "primarily useful," we would say "forget our categories." In other words, we are just trying to use them as a way to facilitate the understanding of the statute.

MR. HERSHMAN: May I ask, then, Mr. Reynolds, if you consider transmitters, which are designed for the purpose of wearing on the body and transmitting to distant locations, prohibited devices?

MR. REYNOLDS: Again you have to examine the particular device. If the device happened to be in a disguised form so that it could be worn right on the clothes, then it would be a prohibited device.

MR. HERSHMAN: What if it is a small device that is worn inside the jacket pocket?

MR. REYNOLDS: From what you have provided me, I would say the answer would normally be "no"; that is that there is not a violation of 2512 absent some other features about it which bring it within 2512. If we are simply talking about a small transmitter, and it is not in any other way adapted for surreptitious use, then I would say it is not a violation of 2512.

MR. HERSHMAN: Well, a device that is designed specifically for the interception of one-party consent monitoring to be worn on a body, out of sight, isn't that primarily useful for the surreptitious interception of oral communications, even though it may be one-party consent communications?

MR. REYNOLDS: Let me say it is very difficult to reach a judgment on a device without seeing the device or having a detailed description.

MR. HERSHMAN: That is the point I am getting at. If you can't decide, how would the manufacturers decide?

MR. REYNOLDS: No, I don't think that is the point! The point is an off-the-top-of-the-head judgment on a device is of very limited utility. But, if you can see the device or gain a full description of the device, I think you can reach a judgment on it. And certainly, the manufacturers and their attorneys are in a position to know every aspect of the device. They know its appearance; they know its uses; they know the way in which it is created. They are in the best possible position to reach a judgment. They are in the same position we are in once we get one of those devices and send it to the FBI laboratory for analysis.

MR. HERSHMAN: Have manufacturers of electronic surveillance equipment approached you or your department and asked for an interpretation of the language "primarily useful"?

MR. REYNOLDS: Yes, there have been.

MR. HERSHMAN: What is your answer to them?

MR. REYNOLDS: We point them to the statute and give them a limited amount of help as to the general nature of the statute. Then we tell them they are in an area where they had best consult with their attorney and let him reach a judgment on whether the particular device they are dealing with or contemplate dealing with is going to violate 2512.

The problem we have in this area is we are not in a position to enter into an attorney-client-type relationship with a manufacturer of electronic devices for the purpose of advising him whether or not a particular device violates the statute. While we haven't had anyone actually come to us with devices in hand—they usually write a letter—some of the manufacturers would like to use us as their attorney as opposed to having a private attorney analyze Section 2512 and apply its standard to the particular device they are interested in.

MR. HERSHMAN: Conversations and testimony of the manufacturers indicate that they want to know no more than if they will be prosecuted if indeed they sell this device to individuals.

MR. REYNOLDS: I think that is very frequently their interest. They are looking for a predetermination on whether or not we will prosecute.

MR. HERSHMAN: Let me turn, Mr. Reynolds, to the proliferation of devices on the market that are primarily useful for the surreptitious interception of wire or oral communications but go under

the guise of burglar alarms, babysitting devices, et cetera; the audio intrusion devices with listenback capability, burglar alarms which one attaches to his telephone and is then able to monitor from any place in the United States. It seems to me that this device has been on the market now for about five years and its only real use is for surreptitious interception. No one can really expect to intercept a burglar's rummaging through a room at the specific time that one calls.

Have you done anything to try to get these off the market?

MR. REYNOLDS: We've got, at present, two cases under investigation involving these devices.

MR. HERSHMAN: When did you initiate them?

MR. REYNOLDS: One initiated back in March and the other initiated more recently.

MR. HERSHMAN: Why this year?

MR. REYNOLDS: This happens to be the time at which advertisements for these devices were called to our attention.

MR. HERSHMAN: But I have advertisements of these devices dating back to 1970 and they are in public magazines and newspapers.

MR. REYNOLDS: This again goes back to what we talked of before, that is whether we have an affirmative action program of reading magazines. I think we have already discussed it at some length.

MR. HERSHMAN: Under what circumstances may a manufacturer of electronic surveillance equipment advertise his wares?

MR. REYNOLDS: Basically, he can't advertise a device that is "primarily useful." Again, we have to focus in on whether it is a device that violates Section 2512. If it does, he can't advertise it. Additionally, neither can he advertise a non-2512 device to be used in a way that would violate Section 2511.

It seems to us that the most a manufacturer can do would be to make known to legitimate purchasers the fact that he has the expertise and has the facilities to create these devices. If such legitimate purchaser is interested in obtaining more information from him, an arrangement can be worked out for the obtaining of that information. In other words, the manufacturer can in effect, leave a calling card as a producer of electronic devices with a law enforcement agency or other agency that would meet the exceptions under 2512 (2).

MR. HERSHMAN: Actually, as I am sure you are quite aware, each and every manufacturer produces a catalog showing the device, listing its specifications and often telling the usefulness of that device.

MR. REYNOLDS: Yes.

MR. HERSHMAN: These catalogs are distributed to law enforcement agencies across the country.

Are you saying that is not proper?

MR. REYNOLDS: No. I would say that to the extent that the distribution is solicited by the law enforcement agency, the distribution of that advertisement would be legal. An unsolicited distribution would constitute a technical violation of the law.

MR. HERSHMAN: In other words, as long as the law enforcement agency requests the catalog first, you feel that would be within the scope of the statute?

MR. REYNOLDS: I would say that would, at least, bring it within the spirit of the statute.

CHAIRMAN ERICKSON: I think at this time we will take a five-minute recess.

We are running somewhat behind schedule but I think we will probably catch up during the noon recess.

[Whereupon, a short recess was taken.]

CHAIRMAN ERICKSON: May we reconvene.

I might say for the record, as people are returning to their seats, this is the last formal hearing that the Commission will have. And the record will remain open at the conclusion of today's hearing, in the event there is a need for submission of additional documents or evidence for the Commission's consideration.

But at the conclusion of today's hearing, the formal testimony that has been taken will have been completed.

Mr. Reynolds, we certainly appreciate your appearing.

I will return your examination to Mr. Hershman.

MR. HERSHMAN: I not only appreciate your appearing here but the fact you are so obviously well prepared for this testimony.

We left off concerning the advertisement of electronic surveillance equipment and we determined that if a law enforcement agency first requested the advertisement from the manufacturer then it would be within the scope of 2512.

It has come to our attention that at least one manufacturer, possibly more, has distributed catalogs to foreign embassies here in Washington, thinking that this is often not on the property of the United States.

What do you say concerning that?

MR. REYNOLDS: I don't construe the statute as permitting such.

MR. HERSHMAN: That would be an illegal act?

MR. REYNOLDS: It would appear to me to be outside the scope of the statute, which would make it an illegal act.

MR. HERSHMAN: You can be assured the Commission will turn over that information to the Justice Department.

Can a manufacturer utilize a distributor to distribute his equipment across the country?

MR. REYNOLDS: I missed an important word in the middle.

MR. HERSHMAN: Can a manufacturer utilize a distributor to distribute his electronic surveillance equipment in the country?

MR. REYNOLDS: When you are talking about a distributor, you are talking about an intermediary?

MR. HERSHMAN: That is correct.

MR. REYNOLDS: No. The statute requires a direct sale from the manufacturer to the authorized purchaser.

MR. HERSHMAN: I might say, Mr. Reynolds, that there are at least a half-dozen distributors that are well known in the country—fairly large distributors—that engaged in just this practice. They purchase their equipment from manufacturers and then re-sell it.

MR. REYNOLDS: Do you have evidence of the purchase and resale of equipment that violates 2512?

MR. HERSHMAN: That is correct.

MR. REYNOLDS: Well, I have invited you, from the time I first met you on the 1st of October last year, to provide us with any evidence you obtained indicating illegality under Section 2511 or 2512.

MR. HERSHMAN: Mr. Reynolds, as you already know, we have given you some material and are prepared to turn over the rest.

I am just afraid with only four attorneys sitting over there you won't have enough to get it through for the next few years.

MR. REYNOLDS: If you had let it trickle in, such a problem would not have arisen.

MR. HERSHMAN: Can manufacturers demonstrate and display their electronic surveillance equipment to authorized agencies?

MR. REYNOLDS: Again, they can demonstrate or display devices under the same condition they could submit advertisements. If it is under invitation from the law enforcement agency or other authorized purchaser, I believe there could be a demonstration. The issue is what constitutes a contract. If there is a contractual arrangement for the development of a sample device for demonstration to an authorized purchaser, it seems to me the ensuing production and demonstration of the device is within the spirit of the law and probably properly within the letter of the law.

MR. HERSHMAN: But if the manufacturer had salesmen cross the country and these salesmen were carrying devices to demonstrate to authorized agencies, would that be a violation?

MR. REYNOLDS: Such a demonstration arrangement would have to be on an instance-by-instance basis. The manufacturer couldn't send out peddlers and let them travel around the country

with devices in their briefcase waiting for the next invitation from a law enforcement agency.

MR. HERSHMAN: Well, I am sorry you missed our hearings on Wednesday, Mr. Reynolds, because we had a manufacturer testify that he does do that.

MR. REYNOLDS: We will make sure we get a copy of that testimony.

MR. HERSHMAN: What particularly bothers me is that we had a manufacturer in yesterday by the name of Martin Kaiser, a Maryland manufacturer, who says he has made the Justice Department aware of violations and nothing has been done.

MR. REYNOLDS: You mentioned that before the hearings. I am unaware of it. I will check and see what I can find. It could be that he has had conversations with the Department prior to the time that I entered my present position. However, I have had one conversation with him in which he complained in general terms about violations on the part of other manufacturers, but he would give me nothing specific. I repeatedly requested information, but he said his business was a very vindictive one and he would be out of business if he supplied information and the word got out. So, to the best of my knowledge, he has not supplied us anything except extremely general allegations.

MR. HERSHMAN: If one manufacturer is allowed to inventory—and we had that testimony on Wednesday, that a manufacturer does inventory—if he is allowed to display his equipment and advertise his equipment more freely than the others, that really is not fair competition, is it?

MR. REYNOLDS: I agree. What you are really talking about is if one manufacturer violates the law and the others don't, do you have an equitable situation? Obviously the answer to that question is "no". We are interested in making sure there is compliance with the statute.

MR. HERSHMAN: Mr. Reynolds, I attended a trade show a few weeks ago across the street from our office in the Washington Hilton. I looked at the exhibits in the show and although I saw no equipment which could be determined to be primarily designed for the surreptitious interception of communications, there was a company who rented a suite in the hotel and who were showing surreptitious equipment to anyone who walked in who could show a shield, a badge, whether he was with the Wildlife and Fish Service or the New York City Police Department.

What is your feeling about that?

MR. REYNOLDS: Based on what you have told me, I would say it appears questionable. I would have to have one other piece of information, and that is whose conference it was and whether this manufacturer was there at the behest of the organization that established the conference.

MR. HERSHMAN: No, he was not.

MR. REYNOLDS: Then it would be difficult under the law to justify what was being done.

Let me say that I was unaware of the particular meeting or convention that you are talking about. However, in a similar instance, in a convention that occurred in the Bahamas about a year ago, we received information in advance that one or more manufacturers were intending to carry devices from the United States to the Bahamas for exactly that type of demonstration. As a result, we instituted an FBI investigation and had FBI agents attend and look for such devices at the conference. We further had the FBI make an effort to obtain information on how the devices got out of the country and how they were returned to the country. So we are interested in that type of situation, and have pursued investigations of such in the past.

MR. HERSHMAN: I believe this particular demonstration or show was put on by the International Association of Chiefs of Police. As I walked into the hotel I was handed a sheet of paper which said "Suite So and So" and showed the name of the manufacturer. I went to the suite and sure enough, there laid out on the table was equipment no one could possibly argue was anything but surreptitious equipment.

Now, I can't believe that in Washington, D.C., with its thousands of FBI agents and thousands of Justice Department people, no one noticed this. I mean, I walked into the hotel and was handed it.

MR. REYNOLDS: All I can tell you is that I received no report of such.

MR. HERSHMAN: While I stood in the room, some police officers—and, as a matter of fact, one of them was rather high-ranking—walked in. They were from a state which did not have a court-authorization statute, and they were very interested in equipment which would be used for wiretapping. I can only assume that no one is looking because if you want to find violations, they are there.

Is there any authority for selling electronic surveillance equipment, prohibited devices, to foreign governments?

MR. REYNOLDS: The basic answer is that we can see one very limited situation in which such a sale could be made, but basically the statute prohibits the sale of devices to a foreign country in that it prohibits the transportation of those devices in interstate or foreign commerce. The two exceptions contained in Section 2512 (2) would allow a communication common carrier and government agencies to possess, transport, etc., proscribed devices in the normal course of their business. The exception also applies to persons under contract to communication common carriers and government agencies.

It is not foreseeable to me that, in the normal course of business, a communication common carrier could engage in a sale of a proscribed device to a foreign country. However, I can conceive of the possibility of an instance arising where in the normal course of business, a federal government agency might enter into a contract for the sale of devices from a United States manufacturer to a foreign government. To the best of my knowledge, it has never been done, but I think the statute leaves open the possibility of its being done.

MR. HERSHMAN: Section 2512 (2) (b) provides an exception for the purchase of equipment for an officer, agent or employee or person under contract with the United States, a state or political subdivision thereof in the normal course of the activities of the United States, a state, or a political subdivision thereof.

Do you have an interpretation of "in the normal course of the activities"?

MR. REYNOLDS: Let me first give one caveat: It is always dangerous to give a blanket judgment as to what is the normal course of business. Obviously, you have to look at each case that arises. However, having said that, let me say that it appears to us as a general rule that a state or local enforcement agency could not, in the normal course of their business, enter into the sale of devices to a foreign government. They simply could use these devices in the normal course of their business devices for legal law enforcement purposes. So long as they use such devices for legal, law enforcement purposes, then they are within the exception in the 2512 (2) (b).

MR. HERSHMAN: As you are probably aware by now, we audited the records of nine manufacturers of electronic surveillance equipment in the United States. These records indicate sale of devices which are primarily useful for interception of communications to states without authorization statutes. Would they have the right to purchase and possess that equipment?

MR. REYNOLDS: The position that I took in my opening written statement was that they could not possess devices that are primarily useful for non-consensual interception of communication.

MR. HERSHMAN: Let us discuss those devices.

MR. REYNOLDS: The non-consensual? The position was they couldn't possess such. However, in a conversation with Professor Blakey before we started the hearing this morning, he pointed out one possible situation in which my analysis might not be totally correct, and I don't deem it wise to argue legislative intent with the person who drafted the statute. So, I would say that there is a possibility of some devices primarily useful for non-consensual interception being legally possessed by a non-

authorization state police department. But, as a general rule, a red flag goes up in my mind if I find there is a non-consensual device possessed by police in a non-authorization state.

MR. HERSHMAN: You indicate you have found a number of instances where this has occurred and you have confiscated the devices in lieu of prosecution; is that correct?

MR. REYNOLDS: Yes.

MR. HERSHMAN: What police departments were those?

MR. REYNOLDS: I can't tell you specifically. Most of these occurred in an earlier time of the statute, before my time in the Department of Justice. But the position taken at the time of these instances was one of seeking voluntary compliance and of providing education. There was always an attempt made to see whether there was any evidence of illegal use of these devices, and in the absence of such evidence we simply went with a forfeiture or voluntary divestiture of devices.

MR. HERSHMAN: The purchase of these devices by police departments would not normally disturb me. However, when I look at the records I see a lot of these devices being sold to regions where there are currently or in the near past have been police wiretapping scandals. I see devices going to Texas, I see devices going to Louisiana, and I see police wiretapping scandals in Texas and Louisiana.

Is it the responsibility of the manufacturer to determine if a police department is authorized to use this equipment?

MR. REYNOLDS: I think the basic responsibility, of course, lies with the police department that would be ordering the devices. I think it would be very difficult to make a case against a manufacturer based on the theory that they must educate themselves as to which states are authorization states and which states are not. However, if we could establish that a manufacturer knew that a state was a non-authorization state and went through with the sale, then I think that we would have the potential of a viable prosecution against the manufacturer.

MR. HERSHMAN: So that the manufacturers must be aware also?

MR. REYNOLDS: No. What I am saying is I don't think we can place an affirmative duty for them to check and see whether it is an authorization state. But, for instance, if one manufacturer has made a sale to a law enforcement agency in Louisiana and then, subsequent thereto, there is some publicity about it or that manufacturer has a conversation with a representative of the Department of Justice and is advised that Louisiana is a non-authorization State, any subsequent sale to an

agency in Louisiana would appear to provide a prosecutable violation of 2512.

MR. WESTIN: I am not sure I understood your position. Are you saying it is not the duty of the manufacturer to know which of our 50 states have passed court-ordered statutes and which have not? Is that some kind of difficult information to acquire and keep up to date on?

MR. REYNOLDS: I don't think it is difficult information to obtain and certainly we would hope and prefer that manufacturers would obtain that information. However, to the extent that they had not, I think that we would have difficulty proving the requisite criminal intent under 2512.

MR. WESTIN: That goes against everything I learned at law school, which is that every citizen has a duty to know what the law is precisely. Are you really saying a manufacturer is not to be charged with the duty of knowing whether a state does or does not authorize court-ordered interception in a universe of 50 states, with reporting that tells us what the law is and newspapers that publicize it?

MR. REYNOLDS: Again, we would prefer, and we would hope that the manufacturers would educate themselves on this point, and I think there has now been sufficient publicity that the education has been accomplished. However, my point is, as we face a particular case, where there has been a sale from a manufacturer to a non-authorization police department, we have to reach a judgment as to whether we prosecute or do not prosecute that particular case. Certainly, if the manufacturer was unaware that the purchaser's state was a non-authorization state, we have a much less severe case than one where there's a very clear, willful violation of the statute. Further, under the *Murdock* standard of willfulness, we would encounter some severe problems at trial if we sought to prosecute such a case.

MR. WESTIN: I would submit that any case in which you were able to present evidence that said that a manufacturer had not informed himself of the state of the law in the 50 states when all the literature of the manufacturers bears usually the imprint "Sold only for use" or other kind of variations on that—I can't believe a manufacturer would get off the hook when that statement appears in the literature and you could show the kind of thing a law student could accomplish in a matter of hours was not done by a manufacturer who was a fulltime professional in the business of selling equipment.

MR. REYNOLDS: Certainly we could argue under *Murdock* that that would constitute a careless disregard for the law. However, it would be a difficult burden for the prosecution to sustain.

MR. WESTIN: I would prefer you started over with something like a crusading spirit to say that you would lay that duty on the manufacturers, rather than having me lead you to say it. It is the matter of your outlook that is going to shape the way the manufacturers go about their duty.

MR. REYNOLDS: I think as a matter of reality, there is now not too much problem in this area. We have had in the last 12 months or so enough publicity as to non-authorization state police departments possessing devices that there is now a fairly good level of education as to which states are non-authorization states.

MR. WESTIN: Thank you, Mr. Hershman.

CHAIRMAN ERICKSON: Proceed, Mr. Hershman.

MR. HERSHMAN: I don't want to limit the problem of the sale of this equipment to local law enforcement. We have also found the sale of surreptitious listening devices to United States Government agencies, agencies who, on their face, would have no need to use this equipment. They don't participate in court-authorized wiretapping.

Should we clarify what "in the normal course of activities" means in this statute?

MR. REYNOLDS: I don't know what particular instances you are talking about in federal agencies. However, if it is not in the normal course of their activities to possess these devices, then the exception contained in Section 2512 (2) which permits possession of proscribed devices is not applicable to them.

MR. HERSHMAN: In the case of the states the manufacturers can well determine whether they have authorization statutes or not. In the case of a federal agency, I am not quite so sure the manufacturers can determine what the normal course of their business is.

Whose responsibility is it to determine that?

MR. REYNOLDS: When you are talking about the federal government, there certainly has to be some self-policing as to which agencies can possess these devices.

MR. HERSHMAN: It would seem to me that the way the statute is interpreted by the manufacturers indicates that they are quite willing to sell any equipment to any government office. Frankly, that is the feedback I get from many of them.

I would like to say there has also been a proliferation of schematics and "how to do it" books on the market. Do you see any illegality in the offering for sale of schematics which depict illegal electronic surveillance devices?

MR. REYNOLDS: It seems to me difficult to bring those within the existing statute. They are very troublesome because they create a do it your-

self situation. However, to bring schematics within 2512, would require the use of a theory of aiding and abetting a 2512 or a 2511 violation.

Let me say, we have recently looked extensively into one case involving the sale of wiring charts for Section 2512 devices to see whether we could develop a theory of prosecution. But, it would be difficult, if not impossible, to sustain this type of prosecution and in the particular instance under consideration, we were unable to develop a prosecutable case. What is clear is that the area is not directly governed by Section 2511 or 2512. If we are going to build a prosecution, we have to resort to an aiding and abetting theory.

MR. HERSHMAN: Mr. Reynolds, on Wednesday we had a panel of manufacturers testify and we discussed the possibility of licensing manufacturers. Most seemed to be in agreement that this might be beneficial in a number of respects.

One, they feel it might in some ways tend to limit the operations of the basement operators who often straddle the post. We have found basement operators who sell equipment to law enforcement but are dealing in the illegal market as well. These manufacturers that we spoke to concerning licensing felt that the licensing might tend to drive these people out; on the other hand, it might tend to drive them totally into the illegal market.

I would like your viewpoint on the licensing of manufacturers.

MR. REYNOLDS: I have a problem coming up with a licensing system that is not unduly burdensome and that is effective. Until and unless we come up with an effective system that doesn't add a great extra level of bureaucracy, I would have to oppose licensing.

However, it is necessary to examine each proposal as it comes up. Right now we are in the process of evaluating a Senate bill sponsored by Senator Percy which has a licensing provision in it. And, it is difficult to make—

MR. HERSHMAN: Perhaps we can turn to a licensing procedure currently in use. In 1974 Canada passed a bill which provides for the licensing of manufacturers. According to the bill, before a manufacturer can sell to an authorized agency, that agency must apply for a sponsor's license to the Solicitor General of Canada. After a sponsor's license is obtained, a manufacturer applies for a seller's license. After the obtaining of a seller's license, he can deal, for a period of up to one year, with that particular law enforcement agency. And he can deal on a contractual basis with them. In other words, during the period of that one year he may sell an unlimited amount of equipment to the agency under contract.

This opens up, of course, the inspection of the manufacturer's records and books for the staff of the Solicitor General. It also seems to perhaps loosen up on keeping inventories. There appears to be some type of suggestion that a limited inventory can be kept, and that demonstration and display can be made without entering into a contractual relationship with an authorized agency.

What about a situation such as that?

MR. REYNOLDS: Do you know what manufacturers this applies to; in other words, what types of devices are included in the licensing agreement?

MR. HERSHMAN: Well, as a matter of fact, the Canadian bill follows our bill very closely in that it describes the type of equipment manufactured as ours does.

MR. REYNOLDS: "Primarily useful." But do they only license the manufacturer who is going to deal in equipment that is primarily useful?

MR. HERSHMAN: Pardon me?

MR. REYNOLDS: Do they only license the manufacturer who is going to deal in equipment that is primarily useful?

MR. HERSHMAN: That is correct.

MR. REYNOLDS: Well, it seems to me that such a licensing provision would be of only limited utility.

The statute still relies on the words that I see the manufacturers complaining about and that is: What is primarily useful for surreptitious interception of communications and what isn't? This is the question which the manufacturers indicate to us is troubling them. They ask for a clearer definition. The licensing provision you are talking about doesn't answer that question. If a manufacturer doesn't apply for a license and markets surveillance devices, you still have the issue as to whether the devices he markets are "primarily useful." Manufacturers who are now complying with 2512 will comply with the licensing requirement and those who are not will not comply.

MR. HERSHMAN: One positive aspect of licensing is that it opens the books and records of these manufacturers. Look what we have done with the books and records of the manufacturers. I think some type of positive program where they could be audited perhaps semi-annually would add to the protections already instituted under the Section 2512.

Do you agree?

MR. REYNOLDS: I would agree that would be very helpful as far as detecting where the violations are occurring, so long as the companies violating the law reflect such violations in their records—something which is very doubtful.

MR. HERSHMAN: Mr. Reynolds, I understand, of course, that you are under certain restrictions in talking about open cases. However, on Wednesday, we received some very disturbing testimony concerning illegal wiretapping in Houston, Texas. During the course of that testimony it was explained to us by the former United States Attorney from Houston and the Chief of Police that federal officers left much to be desired in investigating the allegations of illegal police wiretapping.

Without going into the details of that case, I wonder if you might respond to that.

MR. REYNOLDS: In responding generally, let me focus in on a question you previously asked for in one of the Commission's written inquiries to the Department of Justice: that was, whether the FBI was capable of a good investigation in this area. My answer to that is that I don't see that there is any inherent inability on the part of the FBI or any other federal investigative agency to do a good job in these cases. However, when you ask one police force to investigate another police force, I think the prosecutor has got to keep a closer eye on the investigation than he might keep on other investigations. Further, it is necessary to make sure you don't give investigative responsibility to an agent who has had personal dealings with some of the potential subjects of the investigation. If new subjects are developed who were not anticipated originally, changes in investigative assignments may be necessary to insure that agents are not put in the position of investigating their friends. It is just a matter of being constantly vigilant to insure that we assign investigators who do not have a personal relationship with the people under investigation. And, if that can't be done in the local field office, we can bring in investigators from outside of the area to conduct the investigation.

MR. HERSHMAN: Mr. Reynolds, has the Justice Department undertaken an investigation or study to determine if, number one, the FBI did lack aggressiveness in investigating the Houston affair, and, number two, did you investigate the charges of illegal activities on the part of FBI agents and federal narcotics agents in Houston?

MR. REYNOLDS: The answer to both those questions is yes, and the investigations are ongoing.

MR. HERSHMAN: And there have been no determinations made at this time?

MR. REYNOLDS: Let me explain what I mean when I say "ongoing investigation." First with reference to the way in which federal officials are conducting their investigation that is, is the FBI investigation an adequate investigation? We first seek to make sure that an adequate investigation is being conducted. Once that is determined, however, we

don't drop off at that point. As long as that investigation is continuing, we will continue to watch it very closely and make sure the investigation continues to be properly conducted.

Second, with reference to the allegations being made against federal law enforcement officials to the effect they engaged in illegal electronic surveillance, we take an initial look and reach a determination one way or the other. If the determination is that there have been no violations, we don't drop the matter at that point. Because allegations against law enforcement officials are so serious—and of course we have to be particularly circumspect about allegations against federal law enforcement officials—we continue to watch the matter and continue to look for any evidence of violations by federal officials.

So, I don't mean to indicate when I say the matter is still open that we necessarily have any evidence that indicates a prosecution or indictment will be forthcoming or that there is any evidence of misconduct. It is simply that on something of this magnitude, once we have concluded our initial inquiry we don't close the matter out while the underlying investigation is still going on. We continue to watch it.

MR. HERSHMAN: I think that is a very good procedure.

Have there been any disciplinary actions taken against any federal agents in Houston to your knowledge?

MR. REYNOLDS: As relates to this case?

MR. HERSHMAN: Yes.

MR. REYNOLDS: I don't know. I do know that there have been some changes in assignments as to who conducts the investigation. But as to whether there has been any disciplinary action, I have no further knowledge of any.

MR. HERSHMAN: Can you specify what you mean by changes in assignments? I realize we are dealing in an area that is very uncomfortable at this point because of the ongoing investigation.

MR. REYNOLDS: We have brought in people from outside the Houston area to take a look at the manner in which the investigation is being conducted, and also to evaluate the allegations of improper activity on the part of federal law enforcement agents. When I say "reassignments," I mean that we have been circumspect in trying to bring in agents from outside to beef up the investigation and to make sure that we don't leave it totally in the hands of people who have been in the same area and are acquainted with the primary subjects of the ongoing investigation.

MR. HERSHMAN: Mr. Reynolds, the former United States Attorney in Houston indicated to us

that when he went to the FBI with allegations of serious and widespread illegal wiretapping on the part of the Houston police, the FBI assigned one out of approximately 100 agents within the Houston area office to the case.

Is that normal procedure, would you think?

MR. REYNOLDS: It depends on what the investigative leads are at the time. One agent full-time on a case is not to be considered a meager assignment of personnel. Certainly, at the outset, to determine what the leads are and to gain an initial perspective on the case, I can't say that the assignment of one agent is an unusual procedure.

MR. HERSHMAN: In 1974, the former United States Attorney from Houston, Mr. Farris, wrote a letter to the Attorney General complaining of the lack of aggressiveness on the part of the FBI in investigating the case. Were you made aware of that letter?

MR. REYNOLDS: Yes, I was. I am the one who handled the letter.

MR. HERSHMAN: You handled the letter. Was there a response to that letter?

MR. REYNOLDS: Yes, there was a response to that letter, a prompt response to the letter.

MR. HERSHMAN: While Mr. Farris was there?

MR. REYNOLDS: No, he sent the letter on, I believe, the 17th of December 1974. He was supposed to leave office on December 31st, but physically vacated before that time. The responsive letter went to the new U.S. Attorney Edward McDonough. I believe our letter to him was dispatched on January 7, 1975. Additionally, it had been preceded by telephone calls in which we kept Mr. McDonough apprised of where we stood on the matter.

MR. HERSHMAN: I believe Mr. Farris testified that he had contact with the Justice Department prior to sending that letter and had expressed during that contact his displeasure at the manner in which the investigation was being handled. Do you have any knowledge of that?

MR. REYNOLDS: No, I have no knowledge of that.

MR. HERSHMAN: What did your letter say to the United States Attorney in Houston?

MR. REYNOLDS: I really don't feel that that is appropriate material to disclose at this time. Our letter dealt with the facts and, in part, the strategy for pursuing an investigation which was ongoing at that time and is ongoing now. It dealt with matters that were and are before the grand jury and I think it would be improper to go into the details of such material.

MR. HERSHMAN: We are under the belief that there was a letter in April of 1974 from Mr. Farris

to the Attorney General or to the Justice Department. Are you aware of that letter?

MR. REYNOLDS: No, I am not. Sometime I believe, in the spring or perhaps early fall of 1974, we received a carbon copy of a letter Mr. Farris had sent to the FBI field office in Houston, but that is the only correspondence of which I am aware.

MR. HERSHMAN: What did that letter say?

MR. REYNOLDS: It simply dealt with the facts of the investigation.

MR. HERSHMAN: And it did not in any way express his displeasure with the handling of the investigation to that time?

MR. REYNOLDS: No, no serious overall displeasure was expressed with the investigation in the letter that I am referring to.

MR. HERSHMAN: Any displeasure?

MR. REYNOLDS: There was some contentiousness as to a conversation which occurred between a particular Assistant United States Attorney and a particular FBI Special Agent which was reported in an FBI report. The FBI report indicated that the Assistant United States Attorney had made a certain statement and the letter indicated that the report improperly characterized the conversation.

MR. HERSHMAN: But this was in reference to the Houston wiretapping situation, was it not?

MR. REYNOLDS: This was part of that investigation.

MR. HERSHMAN: Did the Justice Department at that time take steps to determine if there was a problem in the manner in which the investigation was being conducted?

MR. REYNOLDS: There was no problem indicated by that letter. Perhaps I am not referring to the same letter you are.

MR. HERSHMAN: I think you probably are.

MR. REYNOLDS: I am talking about a carbon copy of a letter from the United States Attorney to the Special Agent in Charge of the FBI field office. There was a request that a certain investigation be conducted, and at one particular point there was a correction concerning what one particular Assistant United States Attorney had said to a Special Agent. There was nothing in the letter that was particularly unusual or indicated a problem.

MR. HERSHMAN: Just one further question in this area.

As a result of Mr. Farris' December letter, were any investigative procedures changed?

MR. REYNOLDS: The answer is yes. But that doesn't necessarily mean that we required that changes be made on the method of investigation. Rather we refocused somewhat the way in which the overall investigation was conducted.

MR. HERSHMAN: Would you care to speak about the nature of that refocus?

MR. REYNOLDS: Let me just say that when you are conducting an investigation like the one in question, you have a question as to how much the field investigator can conduct and how much needs to be done within the grand jury room. Our letter focused on how much could be accomplished each place.

MR. HERSHMAN: I want you to understand, Mr. Reynolds, the reason I bring this up is because I feel the allegations that were made on Wednesday are very serious and I feel that Commissioner Blakey made a very good point at that time, that there was no one present to respond to those allegations.

MR. REYNOLDS: I am sorry. I didn't hear you.

MR. HERSHMAN: There was no one present at the Wednesday hearing to respond to those allegations. And I did want to bring the matter out today and give you an opportunity to perhaps shed some light on it.

I just have one other area of interest.

During the late summer of 1974, the Commission received allegations that a Virginia private investigator had been engaging in illegal electronic surveillance. These allegations took the form of a number of tape recordings which I was allowed to listen to. These recordings were made through one-party consent and were made between a local Washington businessman and two employees—one a former employee—of this private investigator.

The tape recordings were somewhat shocking. They indicated a widespread use of illegal electronic surveillance by this private investigator. They detailed the names, the dates, and the types of electronic surveillance that was conducted in at least one case.

We turned this information over to the Justice Department in October of 1974 with the request that it be acted on as soon as possible so that we could possibly follow this situation and use it as a case analysis.

I wonder if you would tell us what the status of that case is now?

MR. REYNOLDS: It is still a pending case.

MR. HERSHMAN: It is still a pending case?

MR. REYNOLDS: That is correct.

MR. HERSHMAN: For the record, I would just like to say I understand it did go to a grand jury in approximately December of 1974 or January of 1975.

One point I would like to make: The businessman who came to me with the tapes still has the tapes in his possession. He has gone to the Justice Department and asked for an informal assurance that his having these tapes and his method of recording these tapes would not lead to his prosecution. I un-

derstand that the Justice Department has refused to give him that assurance and therefore has not received into evidence a very important package, these tapes.

I know you can't comment on an open case, but perhaps you can tell us what the reasoning behind your not receiving the tapes is.

MR. REYNOLDS: I cannot give you the reasoning behind the rejection of an immunity request. However, I think it is a matter of record that the immunity request was turned down. I applied for immunity, and it was denied, and the case is presently proceeding. The fact that we don't have the tapes makes the case much more difficult to develop. It has caused us to work extremely hard and spend a lot of time trying to develop a case, and we are still in that process.

MR. HERSHMAN: One thing about this case which is particularly interesting, and perhaps disturbing, is the fact it was called to our attention that the private investigator who was using the illegal wiretapping was a registered FBI informant. And there have been allegations made that the FBI might have been aware of some of his illegal wiretapping activities.

Has there been an investigation conducted concerning these allegations?

MR. REYNOLDS: Yes, it has been checked out.

MR. HERSHMAN: And can you tell us your findings?

MR. REYNOLDS: I find there is simply no evidence to support that allegation.

MR. HERSHMAN: Not the allegation—I am not suggesting that the individual is a registered FBI informant was an allegation. I think that is an established fact.

MR. REYNOLDS: It is not appropriate for me to comment on whether or not the individual in question had ever supplied information to the FBI. However, I will say that the allegations that appeared in the press back in early October concerning the FBI's dragging its feet because an informant was involved have been thoroughly checked into, and there is just no substance at all to those allegations.

MR. HERSHMAN: I hope the Justice Department will keep us informed as to the progress of this case and perhaps if it is adjudicated before we issue our final report we can still use it as a case analysis.

Thank you, Mr. Reynolds.

MR. REYNOLDS: Let me just say one thing on that. Sometimes a law enforcement agency ends up looking a little ridiculous when asked to comment on ongoing cases. You often receive a lot of comments on the other side while the government sits

there with its mouth shut, looking a little inane about the whole thing. But I think all you gentlemen are aware of the reasons behind our restraining our comments on these and any ongoing cases. Further, I think the case that you have just questioned me on is a perfect example. If I could sit down and let the Commission know step by step exactly what has been done in that case, I think that most of you would agree that it has been thoroughly handled. It will continue to be thoroughly handled.

MR. HERSHMAN: I have no doubt it has been, Mr. Reynolds, and I appreciate that.

I am more concerned about the tapes, the fact that they haven't been obtained. That disturbs me greatly. You mentioned that they are an integral part of this investigation and I see no reason for their not being obtained.

MR. REYNOLDS: When the immunity statute was passed by Congress it vested authority for granting immunity in a relatively high level of the Department of Justice for reasons of uniformity. The determination rests with the people designated in the statute and it is a matter within their discretion. They had reasons for denying my immunity request and I don't have any quarrel with their reasons. After that decision we moved forward to try to develop evidence in other matters.

MR. HERSHMAN: But you had applied for immunity?

MR. REYNOLDS: Yes, that is a matter of record.

MR. HERSHMAN: Thank you very much. You have been very helpful.

CHAIRMAN ERICKSON: Mr. Reynolds, I just have a few questions.

We recognize that this whole area has taken on a complexion, since the term "Watergate" became a national term, that has probably made the public more aware about the uninvited ear than it ever was before or probably ever hopes to be again.

I know my good friend, Professor Blakey, always is a little concerned when I say this statute is a monument to his genius. However, the statute, in my mind is not as clear in some areas as it might be.

The term "primarily useful for interception" leaves means of avoiding the penalties of the act by saying it is for a burglar alarm purpose or for babysitting, when we know very well the purpose of the sale of it is for interception. That part of the statute could probably be clarified, don't you think?

MR. REYNOLDS: I don't think that the subterfuge of advertising an infinity transmitter as a telephone watchman or a burglar alarm device will prevent the government from successfully prosecuting cases involving such devices.

CHAIRMAN ERICKSON: That has been the guise that has been used, hasn't it?

MR. REYNOLDS: Yes, it has been. It is the way that some manufacturers who are willing to market those devices have tried to work their way around the statute.

CHAIRMAN ERICKSON: It really concerns me when we admit that these infinity transmitters are being sold under this ploy and that they can be advertised in every national publication.

When a man testifies as the head of a major detective agency and presents to the Commission an ad from *Playboy* on an illegal device, it seems rather odd that this can go on without any action by the Department of Justice.

And I know, as you said, there is no affirmative action program. But you can't close your eyes and say that something isn't there.

MR. REYNOLDS: Oh, no, we are not. And, as I said earlier, advertisements of two of those devices which have come to our attention are presently under investigation. I foresee a good probability that if the evidence comes out the way I feel it will, a prosecution will follow.

CHAIRMAN ERICKSON: You have mentioned that the size of your staff is approximate to that of the kidnapping and robbery—

MR. REYNOLDS: Their staff is slightly bigger but my analogy was to the fact that, while I might like to have more people, they've got six or seven people, and certainly they would like to have and feel they need more people.

CHAIRMAN ERICKSON: So the problem is that at the present time you have been acting on a complaint basis; isn't that right?

MR. REYNOLDS: Our basic action has been one of responding to complaints.

CHAIRMAN ERICKSON: Has that has been enough to keep you busy? You would not need a larger staff if you didn't have more than you could handle with the work that comes in by way of complaints?

MR. REYNOLDS: We certainly could do more. I don't mean to indicate, though, that an affirmative action program is held up totally because we have only four people. We have the resources of the FBI which are primarily those that would be involved in an affirmative action program. As I said earlier, we have occasionally used affirmative action programs in the past. But we have not routinely had such a program. I just wouldn't preclude the possibility of some affirmative action program being conducted while we stay at our present level of personnel.

CHAIRMAN ERICKSON: The allegations that were made in connection with the Houston scandal, of course, have concerned us very much. Allega-

tions were made that were extremely serious regarding the Federal Bureau of Investigation, and as well about the District Attorney in Houston, whom I respect and have great reason to believe is not only an outstanding prosecutor but a man of the highest intention.

So, for the purpose of the record, I am going to suggest that our investigator contact Carroll Vance, who is the District Attorney from Harris County, and obtain a statement from him, because the Chief of Police of Houston did make a claim that Mr. Vance was notified and did nothing about this and more or less ridiculed the complaint.

[See interview with Carroll Vance, transcript of hearings of Wednesday, June 25, 1975.]

Mr. Hershman, I would appreciate your getting a statement from Mr. Vance regarding that. Because it is only fair that when allegations are made involving a matter this serious, that there be an opportunity to respond. Particularly when you are in the hot seat, if you will, and where the allegations are made after perhaps you have done everything that can be done and are still conducting an ongoing investigation. To allow the allegations to be admitted as proof, if you will, when the proof hasn't been established, is not what this Commission intends to do, at least not while I am chairman.

So we will pursue the facts in this case to try to see that they are developed further. And the testimony which Congressman Kastenmeier took has been included with the Commission's work, and I would have to conclude that is part of the Commission's work because he is a member of this Commission.

Going on somewhat further into the inquiries that were made, when this matter was brought to the attention of the Federal Bureau of Investigation by the Chief of Police, was this made known to the Washington office soon thereafter?

MR. REYNOLDS: I am not sure which contact you are referring to.

CHAIRMAN ERICKSON: When the Chief of Police contacted the special agent in charge of the Houston office.

MR. REYNOLDS: And indicated what?

CHAIRMAN ERICKSON: That there was illegal wiretapping going on within the Houston Police Department; that they had been pursuing these tactics for a long period of time.

What was done? Was Washington notified or was it just left on the local level?

MR. REYNOLDS: It is difficult to respond to that because it comes in the middle of a whole sequence of activities. But basically, we have had an ongoing investigation for some period of time that had, in effect, pyramided—

CHAIRMAN ERICKSON: I am not trying to be critical. I am just trying to ask you—

PROFESSOR BLAKEY: Excuse me. Could I ask one question?

If one brings a complaint to the FBI is it standard practice that they write a 302 report on that complaint—yes or no?

MR. REYNOLDS: Not necessarily a 302.

PROFESSOR BLAKEY: They write it up; right?

MR. REYNOLDS: Yes, unless it is a totally spurious type of thing.

PROFESSOR BLAKEY: And if it is written up, would a copy go to Washington?

MR. REYNOLDS: Yes, a copy goes to Washington regardless, and if it is an interception of communications matter a copy comes to me.

Let me say that I am not trying to be defensive in response to what I feel is criticism. What I am trying to say is that the time frame in which the Chief of Police may have gone to the special agent in charge and indicated he had a problem with his police department was a time frame in which we were already aware of the problem and had an investigation in progress.

CHAIRMAN ERICKSON: So, in short, he wasn't rediscovering the wheel. You knew the wheel existed?

MR. REYNOLDS: That is right.

CHAIRMAN ERICKSON: And an investigation was in progress.

MR. REYNOLDS: And had been for some time.

CHAIRMAN ERICKSON: So there was—

MR. REYNOLDS: That is why it wasn't so striking to me that the chief of police provided information. It was not a line, a dividing point in the investigation. It is just one event in an ongoing investigation.

CHAIRMAN ERICKSON: What I gather is that when the chief of police came in and made his report, that came to the Department of Justice as being as much of a disclosure as the fact that there was Houston, Texas, because you knew that was in existence prior to that time?

MR. REYNOLDS: That is right. It added something but it was no landmark thing. We were already working on it.

CHAIRMAN ERICKSON: And you were glad to have his assistance.

MR. REYNOLDS: The first I learned about it was as part of the attachments to Mr. Farris' letter of December 17th.

CHAIRMAN ERICKSON: You suggested that there be a misdemeanor statute included in an amendment to Title III.

Do you feel that would help in the *Murdock* area in handling a case that really doesn't have felony implications?

MR. REYNOLDS: I think it would give us some flexibility even on the serious violations. At present, our only way to turn a person—that is, to gain the cooperation of a person within a wiretapping conspiracy is through immunity. The preferable practice would be to proceed against such a person with a criminal prosecution, and then seek his cooperation after a conviction or plea. This would give us added flexibility. Additionally, we would add an ability to prosecute cases that are not serious enough to merit felony prosecution.

CHAIRMAN ERICKSON: Fine.

As far as tracing prohibited devices, would it be helpful if there was a requirement in connection with the manufacturer that the devices be identified by serial number?

MR. REYNOLDS: If you are talking about the devices that violate 2512, that would be a good thing. But, again, most of these devices presently being used for illegal electronic surveillance are not devices that violate 2512. Rather, they are readily marketable legal devices. I don't know about the wisdom of requiring serial numbers for your normal commercial electronic devices which could be used for electronic wiretapping or eavesdropping.

CHAIRMAN ERICKSON: The term you have used in connection with liability is "strict civil liability" in connection with Section 2520.

How would you suggest that there be a change in Section 2520?

MR. REYNOLDS: I hadn't proposed a change in Section 2520. My proposal was to add to 2511 a type of strict liability civil penalty, so that regardless of the existence of criminal intent, we would be able to take some form of action against anyone who engages in wiretapping or eavesdropping.

CHAIRMAN ERICKSON: It would be a typical strict liability concept as has been developed in tort law?

MR. REYNOLDS: Let me say that idea is not one that we have had surfaced very long and have had occasion to study in depth. However, as the Department has moved forward, with legislative proposals for civil penalties in other areas of criminal law, it appears to us that an analogous-type provision would be very helpful in the wiretapping and eavesdropping statute. We frequently encounter middle and upper middle class people who have hired private detectives to wiretap. Many of the cases either do not merit felony prosecution or else lack the necessary evidence of criminal intent. Right now our alternative is felony prosecution or nothing. We would like to broaden the alternatives to misdemeanor or felony. Additionally, I think it would be helpful if we had still another al-

ternative: the civil fine. In this way, we would have a viable way to proceed on every instance of wiretapping or eavesdropping.

CHAIRMAN ERICKSON: I am certain every member of the Bureau is aware of the national television show that occurred not too long ago where they publicized a store on New York avenue which was selling certain devices that were apparently violating this law.

Are you aware of that program?

MR. REYNOLDS: Yes, I am. I presume you are referring to the Mike Wallace interview of Justice Department attorney Paul Boucher.

CHAIRMAN ERICKSON: Yes.

MR. REYNOLDS: As a result of the information disclosed in that interview, we immediately had the FBI inspect the shop involved to see whether they did, in fact, possess devices that violate 2512. We found they possessed two devices in violation of 2512, both tie clip microphones. Those devices were seized and have since been forfeited. Further, as a result of that, we proceeded to trace the devices back from that shop to the distributor. We subsequently accomplished a forfeiture of 1,964 tie clasp microphone devices from the manufacturer. We opted to proceed with a forfeiture instead of criminal prosecution since there was a severe question as to the existence of the needed criminal intent. The manufacturer has been totally cooperative and has retrieved from its retailers another thousand-and-some of these devices which it is voluntarily turning over to the FBI.

The devices, incidentally, were manufactured in Japan, so we are not able to take any action beyond the wholesaler of the devices.

CHAIRMAN ERICKSON: Do you have any other suggestions relating to possible amendments of this statute?

MR. REYNOLDS: Yes. I have a number of areas of thought. This doesn't mean we presently have drafted legislative proposals in these areas. However, these are the areas which merit consideration to the extent that legislative changes in Title III are considered.

(1) Misdemeanor, which has been referred to earlier.

(2) The possibility of a civil penalty, just discussed.

(3) Consideration should be given to expanding Section 2511 (1) (c) and (d) to cover the fruits of illegal intercepts. What we find is that there is very often an attorney behind a domestic relations interception. However, we usually don't have sufficient evidence to proceed against the attorney. If the attorney tries to disclose the fruits of the intercept in a trial, such evidence is inadmissible because the

exclusionary rule in 18 U.S.C. 2515 covers fruits of illegal intercepts. However, Section 2511 (1) (c) and (d) do not cover fruits. So I would say we could assist ourselves somewhat by inserting in Section 2511 (1) (c) and (d) an analogous provision to that in Section 2515.

(4) It would be helpful to clarify in the legislative history whether Section 2511 applies to radio waves. The Court of Appeals decision in the *United States v. Hall* 488 F.2d 193 (CA9, 1973), has raised the question whether point-to-point radio communications are, in fact, oral communications. It is a rather technical area of the statute, and one on which we have done extensive research. Our position is that point-to-point radio communications are covered by 47 U.S.C. 605, and that the intent of Congress wasn't to make them a form of oral communication. However, in view of the *Hall* decision, I think that point could use clarification.

(5) I referred earlier to the need to make the service observing exception of Section 2510 (5) a little more specific both as to who can possess service observing equipment and the conditions of its use, to include the requirement that those whose conversations are subject to interception be notified of the fact. I don't think we would be doing more than codifying what we have now and what the telephone companies have in their tariffs. However, I think it would be wise to put the restrictions in the statute.

(6) I would also submit that 2510 (5) (a) (ii) needs to be closely scrutinized. I am frankly not sure what it means. It is the only area of the statute which has stumped us from the start to the present. It is a bit worrisome to have a statutory provision the meaning of which appears uncertain.

PROFESSOR BLAKEY: That is Senator Hart's problem.

CHAIRMAN ERICKSON: It was Senator Hart's problem. It is now the Department of Justice's problem.

MR. REYNOLDS: I am referring to 2510 (5) (a) (ii).

CHAIRMAN ERICKSON: "Being controlled by a communications common carrier in the ordinary course of its business."

MR. REYNOLDS: "or by an investigative or law enforcement officer in the ordinary course of his duties."

PROFESSOR BLAKEY: That is Cary Parker's problem.

MR. REYNOLDS: It has become our problem, so I think there is need for clarification. We can come up with three alternative theories of what that means. However, the legislative history is not sufficiently clear to permit a definitive judgment as to the correct meaning.

PROFESSOR BLAKEY: Cary Parker, for the record, was a representative of the Department of Justice in 1968 and that was a Department of Justice amendment.

CHAIRMAN ERICKSON: I made some accusations against Professor Blakey that I guess he won't have to accede to after all.

PROFESSOR BLAKEY: I liked the genius part, Mr. Chairman. It was just when you got into the drafting that it bothered me.

MR. REYNOLDS: (7) To proceed with possible changes, the next area of consideration would be Section 2511 (2) (a) (i), the toll fraud provision. We haven't gotten into this area in the testimony this morning and it is the area of your next witness, Mr. Caming of AT&T. I don't have a problem with the present toll fraud detection procedures, as I understand them, being used by AT&T affiliates. However, they would be more understandable to everyone and appear less onerous if the legislation specified exactly what the limits of the AT&T power are.

(8) Another area would be to clarify the right of prosecutors to use wiretap tapes against the people who made the tapes and are being prosecuted for the wiretapping. The legislative history indicates that we can use the tapes but the court decisions have uniformly gone the other way.

(9) Turning to the other "injurious act" provision of Section 2511 (2) (d), it seems to me that it needs to be firmed up with more specific language. This of course is Senator Hart's amendment on the floor of the Senate.

CHAIRMAN ERICKSON: Do we need a legislative change to correct the *Simpson* problem?

MR. REYNOLDS: I have no problem with overcoming *Simpson*; we will overcome some day. However, if there were an amendment to the statute before the problem is corrected judicially, it would be helpful to spell out clearly that *Simpson* is just not in line with the theory Congress had in passing the statute.

CHAIRMAN ERICKSON: I think there is no reason to wait for the courts to catch up. I think there should be an amendment.

MR. REYNOLDS: Let me mention that one of the problems we have in overcoming *Simpson* is that often defense counsel will wait and raise the *Simpson* issue after jeopardy has attached. Therefore, if we lose on *Simpson*, we lose it in the form of a motion for judgment of acquittal and have no right to appeal.

(11) Under 2512 and 2513, it seems to me, at least theoretically, Section 2513 incorporates the very difficult willfulness standard and knowledge standard contained in 2512. If there is an amend-

ment of Title III, I think it should be spelled out that the forfeiture statute is a strict liability-type statute.

(12) And as far as the advertisement provision in 2512, I think perhaps it could be made broader instead of being tied to the delineated forms of advertisements. For instance, the statute, as I read it now, wouldn't cover the advertisement of a primarily useful device that might occur on television. That concludes my suggestions. If there are going to be changes in the existing structure, these are all areas that merit consideration.

CHAIRMAN ERICKSON: Well, I think we talked about the problems of 2511 (1) (a) as to whether or not there isn't a question of whether or not a federal purpose is lacking.

MR. REYNOLDS: As relates to oral communications, the problem is not something that Congress can do anything about. It raises a constitutional issue.

CHAIRMAN ERICKSON: I am aware of that, but the language of this might be changed in such a way that the obvious federal purpose could be included.

MR. REYNOLDS: A legislative history change would help because we have in developing our argument to uphold the constitutionality of Section 2511 (1) (a), placed less reliance on Clause 5 of the 14th Amendment, and are using an interstate commerce theory based on the *Perez* decision. The legislative history is designed to support the 14th Amendment argument and, in fact, Congress disavowed reliance on interstate commerce—

CHAIRMAN ERICKSON: Of course the legislative history connected with the amendment would be rather helpful.

MR. REYNOLDS: Surely. It would be helpful if the history expressed a reliance on interstate commerce. Although I think two of the findings included in the existing statute are tied to interstate commerce. Thus, even though there is a disavowing of interstate commerce in part of the legislative history, I think the findings are sufficient that we can make a very respectable argument under the *Perez* rationale.

CHAIRMAN ERICKSON: There is no reason to leave that loophole?

MR. REYNOLDS: No, absolutely not. I think you have raised a good point.

CHAIRMAN ERICKSON: Going on, if amendments were made, what would you think of approaching the emergency wiretap provision somewhat the way the Canadians have in their new act? The emergency provisions have never been used by the Department of Justice.

MR. REYNOLDS: Let me say that you have struck on an area where I have no expertise at all. My work under the statute is limited to the portions containing the criminal sanctions.

Certainly, to the extent you feel there is a need for the Department's position on that, it can be supplied; however, I would not be the person who would have input on that response.

CHAIRMAN ERICKSON: Well, I appreciate your comments on that.

I certainly want to thank you on my behalf for everything you have done for the Commission. I think the Commission is particularly indebted to you for the excellent paper that you have delivered to us for inclusion in our record. It shows the problems that exist today. It is a subject that has been given some careful study by this Commission, by dedicated people, and I hope we can come up with some recommendations that will make the path of law enforcement easier in prosecuting the violations that do occur, protect privacy and at the same time assist law enforcement.

Chief Andersen.

CHIEF ANDERSEN: Thank you, Mr. Chairman.

As you know, I am from Omaha and I think your summarization of the Omaha case is absolutely correct. I notice you did not try the private investigator.

MR. REYNOLDS: Yes. It is a closed case now and I will be glad to say why. The evidence at the trial of the attorney indicated quite clearly that the private investigator resisted supplying and installing the tap. When the attorney said "Put the tap on the line," the private investigator said, "I don't want to get involved. I think there are legal problems." The attorney applied pressure, asserting, "She can put it on her own line. Give her the device and have her install it." In dismissing our case against the attorney, the trial judge summarized the evidence and he found that the private investigator had resisted putting the tap on the line. It appeared to us that once we had lost on the primary subject of the case, the attorney, it would be very difficult to go forward against the private detective who had acted on behalf of the attorney.

Interestingly enough, the trial judge made it clear that his decision on the private detective wouldn't necessarily be the same as the one on the attorney. However, we still felt it would be unwise to go forward. The private detectives were a husband and wife team. We needed the testimony of one of them to support our case against the attorney. We immunized the wife of the private detective team and once immunized she tried in every possible way to cooperate with our prosecution. Based on that cooperation and the trial judge's decision in the

case against the attorney, we felt it was just inappropriate to go forward then with the case against the private detective.

CHIEF ANDERSEN: I have one question that hasn't been discussed here and I would like to have your opinion on it.

I have been reading recently that AT&T over a period of years taped about a million and a half conversations. I am sure you are aware of this, this has been brought to your attention. This is in chasing black boxes, which is a problem of the telephone industry.

My question is: Were any of them turned over to the Justice Department for criminal evidence as far as the gambling is concerned or for other violations?

MR. REYNOLDS: The answer is "yes," but I do not have statistics as to how many. All cases in point that have been decided since Title III was enacted have upheld the right of the government to obtain such information from AT&T. Most recently, *United States v. Clegg* 509 F.2d 605 (CA5, 1975) upheld the right of the government to prosecute a defendant based on information discovered by the telephone company in the course of their toll-fraud monitoring.

CHIEF ANDERSEN: Or for service observing or switchboard observing there are no legal problems so far as turning it over as evidence?

MR. REYNOLDS: We have not had any problems to date and I don't think we will encounter problems. The legislative history indicates that under 2511 (2) (a) (i) the intent is to reflect existing law and cites *U.S. v. Beckley* 259F. Supp. p. 567 (D.C.Ga., 1965). If you look at the *Beckley* case and others like it, decided prior to 1968, it appears that the telephone company does have the right to turn over that type of information, legally intercepted, to law enforcement officials. There was one previous case, *Bubas v. U.S.* 384 E2d 643 (CA9, 1967) that held the other way. However, it hasn't caused us any problems since the enactment of Title III, and with the existing legislative history it should not cause a problem. Accordingly, I think we are on solid ground in receiving such information from telephone companies and in using it in existing trials.

CHIEF ANDERSEN: I have no further questions.

CHAIRMAN ERICKSON: Thank you very much, Chief.

Mr. Westin.

MR. WESTIN: I'm sorry, Mr. Reynolds, I wasn't here at the beginning of your testimony. My plane was late from New York but I have been here more than two hours while you have been answering questions.

I would like to make a statement more than ask you questions. And I think it is fair to say that I appreciate you don't set policies in the Department of Justice since you run an operating unit and some of what I say probably has to be addressed to the policy-making sector, or to Congress or other instruments to try to persuade the Department of justice of the wisdom of what I am going to suggest.

I am very disappointed in the record of the Department of Justice and state law enforcement as well, in dealing with illegal wiretapping by private detectives, individual entrepreneurs and lawless law enforcement officers, because it seems that many of us would call ourselves liberals or civil libertarians without being ashamed of it, who happened to be people who supported the principles of Title III were often derided by our colleagues for being naive and foolish.

We were told we were selling out privacy because we were supporting limited court-ordered wiretapping for specified crimes and under various procedures in the false hope this would lead to extremely vigorous and now dedicated pursuit of lawless, illegal wiretapping.

We were told what would happen would be that law enforcement would use its wiretapping power and we would not really accomplish any effective deterrent on broad-scale illegal wiretapping in the United States; that some people would be prosecuted in the United States; that some people would be prosecuted but there would be a continued loss of confidence in the security of the telephone instrument medium, in the privacy of rooms and in auto conversations, and so forth.

Today we have learned that anyone who reads *Playboy* magazine—and I assume a few in the Department of Justice read that—that anyone who walks along New York Avenue or other streets in the country sees what is done in briefcase and tie clasp and pen and other transmitters being sold.

By picking up magazines other than those in general circulation, *Science* magazine and so forth, we see this kind of open advertising of devices which are in violation of Congress' clear intent, and I would argue of language, in the sections of the 1968 Act, and are faced with this kind of problem. We see enormous expenditures for engaging in wiretapping but we see a unit of small size with a complaint-oriented approach to the resolution of illegal wiretapping activities and the prosecution of wiretap cases.

The problem I have from the very beginning, if I understand what Congress tried to do, at least the compromise of Congress in 1968, it was to have this one area handled, because persons whose conversations are listened to rarely know it. It is not

like burglary, like robbery, like rape, like murder, where the facts come out. The great majority of violations of privacy occur to people without their knowledge. It may come out later, but the harm is done. In the great majority of cases my research informs me it is done without people knowing their business secrets, their private lives, et cetera, have been intruded upon.

So it seems to me we have this very alarming situation in which our Commission has received considerable evidence of illegal wiretapping by law enforcement agencies, or of widespread advertising and dissemination of devices, and so forth, and we see the effort to police the boundaries of the statute is so weak compared to the opening of the barn door to the court-ordered wiretapping, that I think many of us who originally supported the compromise have to look back and say "Have we been had?"

The last three days of our hearings led me to conclude this.

CHAIRMAN ERICKSEN: We will take a short recess.

[Whereupon, a short recess was taken.]

CHAIRMAN ERICKSEN: We will go on for a few minutes. We will try to finish Mr. Reynolds' testimony before the luncheon break, if we can.

We will do the best we can.

Do you remember the question?

[Laughter.]

MR. REYNOLDS: I listened to the comment. I think it would be really presumptuous for me in the time available to respond to each point raised in your comments. Let me simply convey to you that we do have good faith concern about violations of this statute and that we are particularly concerned with the law enforcement violations.

Our hope is that through some legislative changes to 2511 it will be possible to beef up the enforcement of the statute.

I don't mean that to be a response to all the points that you raised. Certainly note is made of your points.

CHAIRMAN ERICKSON: Professor Blakey.

PROFESSOR BLAKEY: Maybe I should ask the witness if he shares my own thoughts about lunch. I don't want to be in the position of holding everybody up from eating. There are several things that I would like to discuss; it probably shouldn't take more than five minutes.

CHAIRMAN ERICKSON: I would say go ahead. I would hope we could probably break by quarter of one, if possible, and if not, we will have to go a little bit more. But we will reconvene at 1:30.

PROFESSOR BLAKEY: Why don't we reconvene—

[Discussion off the record.]

MR. REYNOLDS: I would just as soon proceed.

PROFESSOR BLAKEY: Mr. Reynolds, there has been a kind of interplay here in the discussions of "primarily useful" and the *Murdock* standard of willfulness. Would you support a loosening of *Murdock's* standard of usefulness for the felony prosecution?

MR. REYNOLDS: Section 2511 or 2512 or both?

PROFESSOR BLAKEY: Both.

MR. REYNOLDS: I don't really have any problem with a fairly strict standard of criminal intent for the felony. Whether *Murdock* is the best vehicle or whether there would be some better vehicle for a high standard of criminal intent, I don't know. I personally have trouble with *Murdock* and find it difficult to apply.

But, no, I don't mind a high standard of criminal intent for the felony. When you are in a somewhat regulatory area of criminal law, I can see the merit in not branding as felons people who had no malicious intent; who had no reason to believe their acts would violate the law.

PROFESSOR BLAKEY: If it were possible to draft a definition of a device with mathematical or scientific precision, it might be appropriate to lower the standard. Would you agree that as long as the nature of the beast requires a standard rather than a rule for the definition of a device, there has to be a strict standard on the definition of criminal intent?

MR. REYNOLDS: Right.

PROFESSOR BLAKEY: Given the fact you now have a hard choice between indictment or letting it slide, would it be helpful to you if the explicit language was included in the statute that there be not only civil penalties but a civil injunction process?

MR. REYNOLDS: You mentioned this to me shortly before we started this morning, and I must say it is an area that we have not even given consideration to in the past.

PROFESSOR BLAKEY: I am not too sure that the Department's general power does not already include a right to seek an injunction.

MR. REYNOLDS: I am not, either. That is why I am hesitant to give you a definitive response.

PROFESSOR BLAKEY: In fact, I am inclined to think some of the language in other cases recognizing inherent injunctive power might not be broad enough without new language.

On the other hand, I know there is a sort of natural reluctance to act, of course, unless the explicit language is there.

So what I am really raising with you is: Would it help you in dealing with unfair commercial practices in the area if you could proceed not by forfei-

ture or felony, but by injunction and ultimately, I suspect, by consent decrees?

MR. REYNOLDS: Certainly, as applies to the manufacturers of devices and the inequities that exist, it is one possible way of clearing up any vagueness that might exist in the interpretation of the law.

PROFESSOR BLAKEY: At the same time, do you think it would be helpful if the Department was given specific authority to issue regulations under the statute so that areas are detailed? It could be handled by the Department as a regulatory matter is handled by regulatory agencies?

MR. REYNOLDS: No, I am hesitant to get the Department of Justice into the regulatory area.

PROFESSOR BLAKEY: This is short of making you a regulating agency—short of licensing—if you had an authority to issue regulations under the sections to define certain kinds of common problems administratively rather than through the criminal process or even through a complicated process of civil litigation?

MR. REYNOLDS: It might prove helpful in defining exactly what is primarily useful.

However, you are raising a matter that we have not given much thought to in the past. I would be glad to study any particular recommendation in that regard, and thereafter give you a more definitive response.

PROFESSOR BLAKEY: Let me turn to the Houston matter.

Are you aware of political situations occurring in Houston, apart from this wiretapping, between the Department and that particular United States Attorney?

MR. REYNOLDS: I am aware of some of the background problems that have existed.

PROFESSOR BLAKEY: Am I correct in saying that this is not the only matter of disagreement that the Department has had with that United States Attorney?

MR. REYNOLDS: Are you talking about the former United States Attorney?

PROFESSOR BLAKEY: Yes.

MR. REYNOLDS: My knowledge on that is limited to what I have read in the papers. From that source, I understand that there was one other glaring incident of disagreement between that United States Attorney and the Criminal Division.

PROFESSOR BLAKEY: It is a fact, is it not, there was a problem with immunization of a witness?

MR. REYNOLDS: That is my understanding.

PROFESSOR BLAKEY: And it is a fact that the Department is in litigation over whether a special prosecutor should be appointed in Houston; is that correct?

MR. REYNOLDS: Again, I have really no firsthand knowledge on that prior incident.

PROFESSOR BLAKEY: What I was just raising, to see to it that it is in the record, is that the complaints between this particular United States Attorney and this particular Chief of Police and the Department ought not be seen in isolation.

MR. REYNOLDS: Right. I would agree with that.

PROFESSOR BLAKEY: There has been a continuing problem between the Department and Houston on a number of issues.

Let me ask you another question.

How long does an investigation of this character normally take from the time a complaint is received to indictment? Would two years be an unusual period of time?

MR. REYNOLDS: In what type of case? Are we talking about a law enforcement type wiretapping, violation?

PROFESSOR BLAKEY: Let me give you a hypothetical. We have an allegation of widespread unlawful surveillance by numerous members of a major metropolitan police department. We have a very volatile political situation—new mayors, new chiefs of police, new United States Attorneys. We have allegations of improper conduct on the part of the Department of Justice.

You can reasonably look forward to those allegations finding their way into a criminal prosecution.

Given that general background, would you say two years is too long, as a normal thing, between the beginning of the investigation and the indictment?

MR. REYNOLDS: I would certainly hope normally that a case could be handled more promptly. Certainly we would want to handle it as quickly as possible from the prosecutor's standpoint of having fresh evidence at trial.

PROFESSOR BLAKEY: I take it you would also like to handle it carefully?

MR. REYNOLDS: That is a given. When I say "handle it quickly," I mean as quickly as it is possible to handle it in a careful manner.

PROFESSOR BLAKEY: If you had to choose between speed and care, which would you choose?

MR. REYNOLDS: I would have to go with care.

PROFESSOR BLAKEY: What is the impact on a policeman if he is indicted for unlawful wiretapping?

MR. REYNOLDS: It would vary from police department to police department, but it causes him, at the very least, a lay-off from his employment.

PROFESSOR BLAKEY: He may very well be suspended without pay?

MR. REYNOLDS: I would think that would probably be the normal result.

PROFESSOR BLAKEY: And if you failed to convict him, even though you had some evidence to indicate he had done it, what would be the impact on him?

MR. REYNOLDS: Of course, he has had the period of time that he was laid off.

PROFESSOR BLAKEY: I take it he would also have a criminal record although he would have entered a not guilty plea?

MR. REYNOLDS: Right.

PROFESSOR BLAKEY: It might substantially interfere with his progress, his home life, his happiness?

MR. REYNOLDS: I don't think there is any doubt about it. What you say argues for both care and speed. We are particularly concerned with care in the pre-indictment stage so that we don't indict people who we don't have a very solid, prosecutable case against.

PROFESSOR BLAKEY: What is the impact in the community when a public corruption case such as a wiretapping case is brought and then lost? Does the Department's credibility suffer?

MR. REYNOLDS: The Department of Justice?

PROFESSOR BLAKEY: Yes.

MR. REYNOLDS: I don't know. I suppose in the eyes of some it would suffer.

PROFESSOR BLAKEY: I suppose it would suffer both in the eyes of those who felt it should have been won and those who felt it shouldn't have been brought; is that right?

MR. REYNOLDS: Right. It might tend to feed the dismay of both sides with the Department.

PROFESSOR BLAKEY: So it is true that by losing these cases you lose with everybody whereas by winning these cases you lose only with some people?

MR. REYNOLDS: Yes.

PROFESSOR BLAKEY: I raise these things, Mr. Reynolds, so that the record will reflect what I thought day before yesterday.

When I heard the testimony from the United States Attorney and the Chief of Police it seemed

to me, if I may make a personal statement on the record, that however well motivated, it was at least ill-considered until a reasonable period of time had passed before the Department had had an opportunity to play out whatever it needed before it acted. And it seems to me the jury is still out in the Houston area.

On the other hand, I wouldn't want you to construe anything I have said here as condoning a lack of action on the part of the Department in the Houston case. I would hope that you act with all deliberate speed, consistent with care in that area.

MR. REYNOLDS: I think when the record is available, after the fact, it will be clear that the Department of Justice has done a very conscientious and, I think, solid job in this case.

However, I think the point you raise is well taken. Certainly, any comments made by public officials during the pendency of an investigation just aggravate the situation and cause additional damage to the possible subjects of the investigation.

PROFESSOR BLAKEY: Mr. Reynolds, I would like to insert in the record my thanks to you for a very able, very articulate and very sensitive understanding of a very complex task and, as the Chairman observed, maybe if Title III was a little better drafted, you wouldn't have had to work so hard.

But you are to be congratulated for laboring sometimes with a very heavy oar.

MR. REYNOLDS: Let me just say Professor Blakey, your name has been very much in my vocabulary and on my mind for two years now. There were a few times when I stopped just short of calling Cornell to see whether Professor Blakey was available to discuss the statute. We even gave consideration in one case as to whether you would be an appropriate expert witness. I appreciate this opportunity of meeting you.

CHAIRMAN REYNOLDS: We will incorporate into the record your full statement with accompanying documents.

[The prepared statement of James Reynolds, including accompanying documents follows.]

Mr. Chairman and distinguished members of this commission. I appreciate the opportunity to appear before you today to discuss the experiences of the Department of Justice in the enforcement of the sanctions against illegal electronic surveillance contained in Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

During the seven years which have passed since the enactment of the statute, the Department has encountered a diverse assortment of factual situations which have required our interpretation and application of most every aspect of Sections 2510 to 2512 of Title 18, United States Code. That experience has provided us some insight into the existing difficulties in enforcing the statute. I would like to review for you the focus of our enforcement program, with particular attention given to some of the more significant problems which have been encountered and to suggestions for legislative amendment of the statute.

TITLE 18, UNITED STATES CODE, SECTION 2511

Prosecutive Policy:

Section 2511(1) contains a blanket prohibition against the interception of any wire or oral communication and the knowing disclosure or use of the contents of such an intercepted communication. The Department's overall prosecutive policy under this section has been to focus primarily on persons who engage in or procure illegal electronic surveillance as part of the practice of their profession or incident to their business activities. This includes private investigators, attorneys, law enforcement officials, and business executives. Less emphasis is placed on the prosecution of persons who, in the course of a transitory situation, endeavor to intercept communications on their own, without the assistance of a professional wiretapper or eavesdropper. This does not mean that such persons are never prosecuted, but simply that this type of prosecution is not a major thrust of the Department's enforcement program.

Our experience has been that most illegal interceptions fall into one of five general categories: (1) domestic relations (including intercepts incident to relationships between husband and wife, parent and child, and paramours); (2) industrial espionage; (3) political espionage; (4) law enforcement; and (5) intrabusiness (including intercepts incident to dealings between management and labor, a business and its customers, and rival factions of management or labor). The preponderance of interceptions are in the

domestic relations category. Although we do not maintain statistics in this regard, we would estimate that upwards of 75% of all violations are motivated by domestic relations disputes. The remaining violations are widely spread among the remaining categories.

Consistent with our prosecutive policy, reports of violations in the industrial espionage, political espionage, law enforcement, and intrabusiness categories receive intensive investigation. Law enforcement violations are of particular concern because of the doubt they cast on the integrity of our system of justice.

By contrast, the primary emphasis in the investigation of violations which appear to fall in the domestic relations category is on determining whether the interception (or endeavor) was facilitated by a professional wiretapper or eavesdropper, or by devices proscribed under Section 2512. If there is evidence of the participation of a private investigator, moonlighting telephone company technician, attorney, or other professional, the investigation is continued in an effort to build a successful prosecution. Similarly, if a proscribed device was used, every effort is made to identify and prosecute its manufacturer and supplier. However, where the evidence indicates that the act was perpetrated by a family member, using a crude device not proscribed by Section 2512, we generally do not proceed with a prosecution. Further, in those instances where one spouse hires a private investigator to conduct electronic surveillance on the other spouse, the Department usually foregoes the prosecution of the offending spouse in favor of using his or her testimony to build a prosecutable case against the private investigator.

The Department's policy in this regard has its underpinning not only in the efficient allocation of limited resources but also in the standard of willfulness embodied in Section 2511. The legislative history of that section defines "willful" by citing United States v. Murdock, 290 U.S. 389 (1933). Senate Report No. 1097, 90th Congress, 2d Session, page 93 (1968). That case defines willful to mean an act done with a bad purpose or evil intent. Further, the court in Murdock cited approvingly decisions which defined willful in terms of "a thing done without ground for believing it lawful" and "conduct marked by careless disregard whether or not one has the right so to act." In a prosecution against a family member for domestic relations electronic surveillance, it is often difficult or impossible for the Government to sustain its burden of proof under this definition of willful. This

is especially true in the face of the frequently repeated view that it is legally permissible for a spouse to engage in electronic surveillance within his own home or on his own telephone.

A long range goal of the Department's policy on Section 2511 has been the eventual transfer to the states of prosecutive responsibility for electronic surveillance violations which do not have significant interstate ramifications. This policy would have its greatest effect on domestic relations cases, as a substantial percentage of that category of violations have little, if any, federal interest. In an effort to facilitate this concept of shared prosecutive responsibility, we have actively encouraged the states to enact proscriptions against electronic surveillance. Numerically, the results have been gratifying. At last count, 32 states and the District of Columbia had passed laws prohibiting both wiretapping and eavesdropping. Another 11 states have statutes forbidding wiretapping. Unfortunately, however, many of these states do not appear to be utilizing their statutes. Our attempts to refer cases of questionable federal interest to state prosecutors have met with little success.

Problems Encountered in Enforcement:

1. Constitutionality of Section 2511(1)(a) as Applied to Eavesdropping Violations: The existence of this constitutional issue is thoroughly documented and analyzed in the legislative history of the statute. See Senate Report No. 1097, supra, page 92; Hearings before the Subcommittee on Administrative Practice and Procedure of the Senate Judiciary Committee, 90th Cong., 1st Sess., on the Right of Privacy Act of 1967, Part II, p. 441 et seq. We are generally able to avoid the constitutional question by prosecuting eavesdropping violations under one of the delineated categories of Section 2511(1)(b) which has an established connection to interstate commerce. Our experience to date indicates that only rarely are all of the categories of 2511(1)(b) inapplicable to a given act of eavesdropping, and thus resort to 2511(1)(a) necessary. However, the Department is presently involved in the prosecution of such a case. Predictably, the case is now on appeal to the United States Court of Appeals for the Fourth Circuit with the key issue being the constitutionality of the blanket eavesdropping prohibition contained in Section 2511(1)(a). If the court's decision reaches the constitutional issue, it will represent the first appellate determination in this regard.

2. Noncomplaining Victims: Illegal electronic surveillance is a crime which often produces noncomplaining victims. To the extent that the surveillance goes undetected, its victims are unaware that they have been the subject of a crime. Moreover, in instances of domestic relations electronic surveillance the victims frequently choose not to lodge a complaint for fear that the ensuing investigation and trial will focus attention on their own indiscretions. As a result, the reporting of such violations is often dependent on their fortuitous discovery by a disinterested party, such as a telephone repairman.

3. Uncooperative Witnesses: The clandestine nature of unlawful electronic surveillance presents a formidable obstacle to successful investigation. Usually, devices discovered are not traceable, and — in the absence of a chance observation of the violator installing or attending his equipment — success in making a case often depends primarily on obtaining the full cooperation of the victims and one of the violators.

In contrast to what might be expected, victims are often unenthusiastic about assisting prosecutive efforts. This reluctance is reflected in the extremely infrequent use which is being made of the civil remedies portion of Title III, Section 2520 of Title 18, United States Code. It appears to be based on the fear that the content of intercepted statements will become public if an investigation and trial are pursued. As reflected above, the most extreme opposition from victims is encountered in cases of domestic relations surveillance where the victims fear exposure of indiscretions. In a recent case a victim of an illegal intercept apprised this Department in no uncertain terms that he would do everything possible to thwart a prosecution. He appealed for the discontinuation of our investigation, stating that a prosecution would do far greater violence to his privacy than did the illegal intercept.

Grants of immunity can be of considerable assistance to us in obtaining the testimony of one of the violators if we have developed enough independent evidence to prevent the immunized witness from taking all responsibility on himself, thus exculpating others involved. When needed, an immunity is generally sought for the least culpable violator. However, such witnesses are frequently uncooperative and of very limited assistance to the Government.

4. Difficulty in Establishing Willfulness: The Murdock standard of willfulness discussed above poses a substantial impediment to the successful prosecution of persons who violate Section 2511. It plays a significant role in our determination of which cases will be pursued. Otherwise provable violations (especially those by nonprofessionals) sometimes present fact situations which, in light of Murdock, cannot in good faith be prosecuted.

5. The Court of Appeals Decision in Simpson v. Simpson: In Simpson v. Simpson, 490 F.2d 803 (CA5, 1974), cert. denied 43 U.S.L.W. 3239 (U.S., Oct. 22, 1974) the Fifth Circuit held that the civil remedies portion of the federal electronic surveillance statute (18 U.S.C. 2520) does not allow recovery by a wife in a suit against her husband for wiretapping by the husband of the phone in the couple's marital home. Unfortunately, the decision inferentially and in dicta indicates that such interspousal wiretapping is not a crime. This represents a significant inroad into the blanket prohibition contained in Section 2511.

The court in Simpson conceded that the clear wording of the statute appears to proscribe such wiretapping. However, in deference to the traditional interspousal immunity from tort actions, the court undertook a search of the legislative history of the statute to determine if Congress had specifically expressed a desire to apply the statute to interspousal wiretapping. Finding no controlling expressions of legislative intent, the court hesitantly reached its decision, stating in so doing that "we are not without doubts about our decision" and "our decision is, of course, limited to the specific facts of this case." Simpson v. Simpson, supra, at 810.

The relevant legislative history uncovered by the court is set forth in a footnote to the decision. Unfortunately, the court did not locate portions of the legislative history which indicate explicitly that the proscriptions of Section 2511 are designed particularly for applicability to electronic surveillance conducted in domestic relations and industrial espionage situations. In view of such expressions of Congressional intent, the Department has not altered its prosecutive policy to conform with Simpson. We have on several occasions since the Simpson decision prosecuted a spouse for electronic surveillance conducted within the marital home. However, no additional law has been developed on this issue as the defendants have not raised the Simpson issue.

The main difficulty encountered as a result of Simpson has been its derivative effect on the element of willfulness. In prosecutions brought against attorneys and private investigators for involvement in electronic surveillance emanating from marital disputes, the Government is occasionally encountering the argument that the defendant relied on Simpson in advising a client to wiretap or in carrying out the wiretap for the client, and thus did not willfully violate Section 2511. This argument can cause serious problems for the prosecution in view of the Murdock standard of willfulness and the fact that this argument is generally raised in the form of a motion for judgment of acquittal, thus allowing the prosecution no appeal from an adverse decision by a trial judge.

6. Judicial Nullification: On several occasions United States District Court judges have been openly defiant of Government efforts to prosecute Section 2511 violations. More common, however, are expressions of judicial distaste for prosecutions emanating from marital disputes, an attitude which sometimes appears to inure to the benefit of the defense. Doubts have been expressed as to whether U. S. District Court is the appropriate forum, and a felony prosecution the appropriate medium, for disposition of domestic relations wiretapping and eavesdropping cases. Such judicial distaste has resulted in incidents of trial judges' urging the Government to dismiss; to acquiesce to nolo contendere pleas; to dismiss in favor of a guilty plea to a inapplicable misdemeanor (in our view there is no federal misdemeanor charge applicable to private acts of illegal electronic surveillance); and to dismiss in favor of a state misdemeanor prosecution.

7. Jury Nullification: Again, this problem is particularly critical in prosecutions resulting from marital disputes. One strongly suspects that in such prosecutions the Government is sometimes viewed by jurors as the defender of persons caught in immoral conduct. In some cases, there may be a tendency to consider the results of the given instance of electronic surveillance as vindicating its use.

Consideration of Legislative Changes:

1. The Need for an Alternative to Felony Prosecution: At present, the only alternative provided by federal statute to a felony prosecution under Section 2511 is the forfeiture under

Section 2513 of the device used to accomplish the intercept. (There appears to be one exception; in the case of an illegal interception by a law enforcement officer, 18 U.S.C. 242 (deprivation of rights under color of law) appears to be a viable misdemeanor charge). The forfeiture provision is a helpful supplement to Section 2511, but hardly provides a suitable alternative. Legislation amending Section 2511 to create (1) a misdemeanor violation with a general criminal intent standard (mens rea), and (2) a strict liability civil penalty, would go far toward permitting a fairer and more effective prosecutive program against illegal interceptions. The Department has not yet completed the detailed study of these suggestions necessary for our final endorsement of such legislation. However, it is felt that these proposed alternatives merit serious consideration.

2. The Need to Expand the Scope of 18 U.S.C. 2511(1)(c) and (d): Our experience with the enforcement of Section 2511 over the past seven years has led us to conclude, albeit reluctantly, that attorneys bear a significant burden of the blame for the continued use of illegal electronic surveillance. We have seen repeated instances of attorneys in domestic relations cases using the fruits of illegal interceptions either as evidence at trial or as a means of obtaining a settlement. In many of these instances, the nature of the evidence used has been such that it is difficult to believe that the attorney failed to appreciate its origin.

The only risk the attorney runs in the use of such evidence is that it will be deemed inadmissible in accordance with the provisions of Section 2515. The criminal sanctions contained in Section 2511(1)(c) and (d) apply only to the knowing disclosure and use of the contents of illegally intercepted communications. They are not applicable to the disclosure or use of the fruits of illegal interceptions. To the extent that attorneys are willing to use such evidence, the task of obtaining statutory compliance by private investigators is made more difficult. Accordingly, consideration should be given to the extension of 2511(1)(c) and (d) to cover the knowing disclosure and use of the fruits of illegal interceptions. Such a statutory change would probably not lead to a great number of additional prosecutions as the element of knowledge would be difficult to prove. However, the threat of a prosecution should serve as a valuable and needed deterrent.

3. Applicability of Section 2511 to the Interception of Radio Communications: The overall thrust of Title III and its legislative history seems to indicate that the statute treats radio transmissions as a facet of communications separate and apart from wire and oral communications. Under this view, the interception of point to point radio communications would be governed exclusively by 47 U.S.C. 605. However, confusion is created by the apparently anomalous reference in Section 2511(2)(b) to "oral communication transmitted by radio." Citing that provision, the Court of Appeals for the Ninth Circuit has held that point to point radio communications are a form of oral communication and thus are within the purview of Section 2510 and 2511. United States v. Hall, 488 F.2d 193 (C.A. 9, 1973). In any future amendment to Title III, attention should be given to the clarification of this issue, and to an overall re-examination of the efficacy of applying any of the proscriptions of Section 2511 to the interception of radio waves..

4. Service Observing: Service observing of the telephone conversations of company employees by management may be permissible under two different provisions in the statute. First, Section 2510(5) essentially exempts from the criminal provisions of Section 2511, interceptions of communications made by "any telephone . . . instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a communications common carrier in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business" The legislative history of the provision indicates that it was intended to include service observing equipment. See testimony of Hubert L. Kertz, Vice President of Operations, American Telephone and Telegraph Company in Hearings on the Right of Privacy Act of 1967 Before a Subcommittee of the Senate Committee on the Judiciary, 90th Cong., 1st Sess. 586-88 (1967). The key issue under this provision is whether a company's interception of its employee is in the "ordinary course of business." There is no requirement that the employee be advised that he is subject to such interceptions.

Second, service observing can in some instances be justified under the consent provision contained in Section 2511(2)(d). Consent may be express or implied. Senate Report No. 1097, supra., p. 93-94 (1968). A study of implied consent in terms of the interception of communications statutes indicates that a two-pronged test needs to be met: (1) sufficiency of the interest of the intercepting party, and (2) notice of the interception. Cf.

Blakey & Hancock, A Proposed Electronic Surveillance Control Act, 43 Notre Dame Lawyer 657, 663 n.11 (1968); Brandon v. United States, 382 F.2d 607 (C.A. 10, 1967). Under this test it would appear that an airline, for example, has an interest in assuring that its customers receive proper and courteous service from its personnel who handle incoming calls. In that situation, service observing would appear to be legally permissible as long as the affected employees are notified in advance that they are subject to interception.

There appear to be substantial policy reasons which favor the continuation of the second category of service observing. Employers have a legitimate interest in the conduct of their employees toward potential clientele. Further, the onerous aspects of such interceptions are substantially reduced by the fact that the employee must be put on notice that his conversations are subject to interception, and thus he no longer has an expectation of privacy in such communications. The first category of service observing — that sanctioned by Section 2510(5) — is, however, more difficult to justify. The employee need not receive any notice of impending interceptions. Further, the decision concerning who can obtain service observing equipment is left solely to the discretion of the communication common carriers. This seems inappropriate. The implied consent rationale appears to provide sufficient latitude to management to engage in service observing. Serious consideration should be given to redrafting Section 2510(5) to remove or limit the portion of it providing for service observing. Further, the limits of implied consent service observing should be set forth definitively in the statute.

5. Use of the Contents of Illegal Electronic Surveillance Tapes Against the Perpetrator of Such Surveillance: Section 2515 of Title 18, U. S. Code, prohibits the use of the contents of illegally intercepted communications as evidence in judicial proceedings. No exception is contained on the face of the statute for the use of such contents, when necessary, as evidence in a prosecution against the interceptor. However, the Senate Report on Title III indicates in its discussion of Section 2517 that an investigative or law enforcement officer can, in limited situations, disclose and use illegally intercepted communications. The Report goes on to cite as an example of such a situation the investigation and prosecution of an illegal wiretapper. Senate Report 1097, supra, pp 99-100. Notwithstanding this legislative history, the courts

have not permitted the prosecution to use illegally intercepted communications against the interceptor, absent the consent of the victims. United States v. Bragan, 499 F.2d 1376 (CA4, 1974); United States v. Newman, 476 F.2d 733 (CA3, 1973); United States v. Liddy, 354 F.Supp. 217 (D.D.C., 1973), rev'd, 12 Cr. L. 2343 (Jan. 19, 1973). Although the Government's case is usually not dependent on the illegally made tapes, a situation could arise in which the admissibility of selected portions of the tapes is of critical importance. In that limited situation, the balance of relevant interests appears to weigh in favor of their admissibility. In any future amendment to Title III, attention should be given to the clarification of this issue.

6. Difficulties of Interpretation in 18 U.S.C. 2511(2)(d): Section 2511(2)(d) permits persons not acting under color of law to intercept a communication where one of the parties to the communication has given prior consent, unless the communication is intercepted for the purpose of committing a criminal or tortious act "or for the purpose of committing any other injurious act." That final phrase of the subsection creates problems of interpretation. There is scant legislative history to explain its intended meaning since Section 2511(2)(d) was added to Title III as a floor amendment. Brief Congressional pronouncements indicate that the overall intent behind the added section is to make the one party consent exception available only for "private persons who act in a defensive fashion" 114 Congressional Record 14694 (May 23, 1968). The only example provided of a noncriminal or tortious intent to injure is the secret, one party consent recording of a conversation for the purpose of "publicly embarrassing" the nonconsenting party. 114 Congressional Record 14694. Some further light is shed on the meaning of the statutory provision by the delineation of two types of one party consent interceptions which are not prohibited: (1) a recording made of "information of criminal activity by the other party with the purpose of taking such information to the police"; and (2) a recording made out of a "legitimate desire to protect himself and his own conversations from later distortion . . . by the other party." 114 Congressional Record 14694.

This Department has never sought to base a prosecution on the instant statutory provision, i.e., a one party consent recording made for the purpose of committing a noncriminal or tortious injurious act. However, there are certainly some equitable wrongs for which no criminal or tort remedies are available.

While it remains possible that a suitable, flagrant situation might arise where the Department would institute a criminal prosecution based on the instant statutory provision, it appears unlikely that the provision as presently drafted can play a significant role in the Department's enforcement program. Any amendment of Title III should consider the redrafting of the phrase "other injurious acts" to include a more specific statement of the scope of the prohibition.

TITLE 18, UNITED STATES CODE, SECTION 2512

Prosecutive Policy:

Section 2512 essentially prohibits the manufacture, possession, sale, and transportation in interstate or foreign commerce of devices primarily useful for the surreptitious interception of communications unless done by an agent of a communications common carrier, an agent of a governmental unit within the United States, or a person under contract with such carrier or government. The starting point in developing a prosecutive policy under this Section must center on the Congressionally intended meaning of the term "primarily useful for the purpose of the surreptitious interception of . . . communications." The legislative history of the statute makes it clear that it is designed to prohibit "a relatively narrow category of devices whose principal use is likely to be for wiretapping or eavesdropping." Senate Report No. 1097, 90th Congress, 2d Session, page 95 (1968). From the examples delineated in the Senate Report, it appears that the devices proscribed by the statute are of two basic types: (1) disguised listening devices, and (2) devices designed to intercept communications occurring elsewhere than the location of the interceptor. Senate Report No. 1097, supra. As long as the statute is strictly applied to those two types of devices, there appears to be a reasonable basis for determining whether a given device is primarily useful for the surreptitious interception of communications.

The statute is not, however, designed to and does not have the capability of preventing the possession and distribution of all electronic devices which may prove of assistance to wiretappers and eavesdroppers. Further, the statutory proscription of all such devices does not appear feasible as it could only be accomplished at the cost of prohibiting the manufacture and possession of many normally innocuous electronic devices which are in common usage today. For example, the miniature microphone-transmitter and the

voice actuated tape recorder with telephone relay are highly useful devices in the hands of a would-be wiretapper or eavesdropper. However, such devices cannot per se be deemed to be primarily useful for the surreptitious interception of communications since they are widely used in the electronics industry for legitimate and nonsurreptitious purposes. The smallness of a device and its adaptability to use for interception will not suffice to bring it into the category of a proscribed device in the absence of attributes which give predominance to the surreptitious character of its use, such as an operating feature that has little utility in nonsurreptitious use or a disguised shape which has no operational utility. Senate Report No. 1097, supra., p. 95.

Our prosecutive policy is, as it must be, shaped to the reality of the inherent limitations of Section 2512. We conscientiously strive to preclude the manufacture, possession, sale, advertisement, and transportation in interstate or foreign commerce of devices which fall within the proscriptions of the statute. However, we have no illusion that such action on our part eliminates the availability of electronic gear useful for illegal electronic surveillance.

In our contacts with manufacturers who seek to produce prohibited devices for sale to the narrow category of authorized purchasers set forth in Section 2512(2), we have been consistent in our admonitions that: (1) they may not advertise prohibited devices or promote the use of devices for surreptitious interception; (2) they may not manufacture and stock for inventory in anticipation of making a permitted sale; (3) sale to another supplier for resale to an authorized purchaser is prohibited; (4) there is no authority for direct sale to foreign governments; and (5) they may not demonstrate working samples of prohibited devices or furnish information thereon except in response to specific request or inquiry from an authorized purchaser.

When apparent violations of Section 2512 are uncovered we consider the alternatives of pursuing a criminal prosecution or simply forfeiting under Section 2513 the devices involved in the violation. When there is no evidence that the perpetrator of the offense has engaged in other violations and where the desired deterrent effect will be adequately achieved, we may forego the criminal prosecution in favor of a forfeiture.

Problems Encountered in Enforcement:

1. Difficulty in Establishing Willfulness: Once again the Government is confronted with the burden of establishing criminal intent consistent with the Murdock case, previously discussed. This difficult obstacle to a successful prosecution is buttressed by the requirement that we establish that the offender knew or had reason to know that the design of the device rendered it primarily useful for the surreptitious interception of communications. Further, this same standard of knowledge and intent must theoretically be met to accomplish a forfeiture under Section 2513. Under that statute we must establish that the device was used in violation of Section 2511 or manufactured, possessed, transported, sold, or advertised in violation of Section 2512. This has the effect of incorporating into the civil forfeiture provision the Murdock standard of willfulness.

2. Relationship of Exceptions Contained in Section 2511 to the Prohibitions of Section 2512: The legislative history of Section 2512 appears to provide clear indication that devices primarily useful for the surreptitious interception of communications violate the statute regardless of whether their primary surreptitious function is legal or illegal under Section 2511. This is implicit in the delineation in the Senate Report of cuff link and tie clip microphones as proscribed devices. Senate Report 1097, supra, p. 95. Such devices have their utility in one party consent interceptions which are generally permissible under Section 2511(2)(d). Despite this expression of Congressional intent, some courts have been reluctant to apply Section 2512 to one party consent intercepting devices. United States v. Bast, 348 F.Supp. 1202 (D.D.C., 1972); vacated 495 F.2d 138 (1974); United States v. James A. Six, D.C.N.D. Indiana (1970). This problem was somewhat alleviated by the Court of Appeals decision in Bast which supports our interpretation of the legislative history. However, the view that the exceptions of Section 2511 are incorporated into Section 2512 is often repeated and still appears to be an obstacle to the clear perception of the proscriptions of Section 2512.

3. Possession of Proscribed Devices by Police Departments in Non-Authorization States: As a general statement, as long as proscribed interception devices are used by governmental police agencies for a legal law enforcement purpose, the exception contained in Section 2512(2)(b) is applicable and the prohibitions of Section 2512(1) remain inactive. Once the equipment is used

either illegally or for other than a law enforcement purpose, resort to the statutory exception is lost, and the provisions of Section 2512(1) are activated, making possession illegal.

If a state has no authorizing statute for the purpose of meeting the requirement of 18 U.S.C. 2516(2), it cannot be in the normal course of activities of state and local police departments in that state to intercept communications without at least one party consent. Accordingly, it cannot be in the normal course of their activities to possess equipment primarily useful for the nonconsensual interception of communications. However, one party consensual interceptions are permissible under the federal electronic surveillance statute if intercepted "under color of law," 18 U.S.C. 2511(2)(c). So long as such intercepts are permitted under state law, the state and local police may legally engage in one party consent intercepts. Since such intercepts would then be both legal and for a law enforcement purpose, the equipment used is exempted from the prohibitions of Section 2512(1).

Accordingly, even though the state is a "non-authorization state" it would be legal for police departments to possess those devices proscribed by Section 2512(1) which are designed for one party consent interceptions. It would not, however, be legal for them to possess devices designed for nonconsensual interceptions. We have encountered several instances where police forces in non-authorization states have been found in possession of offensive (nonconsensual) electronic surveillance equipment. Where our inquiry has revealed no evidence of the use of such equipment, we have foregone criminal action in favor of divestiture of the equipment in question. However, any evidence of illegal use is vigorously investigated for the purpose of criminal prosecution.

Consideration of Legislative Changes:

1. The Licensing of Manufacturers: Correspondence sent to the Department earlier this month by the Executive Director of your commission broached the subject of licensing manufacturers of Section 2512 devices. While the Department does not want to prejudge any specific licensing proposal which might later be submitted for our scrutiny, it should be noted that we have grave reservations as to the viability of the concept. The starting point of any licensing system is the defining of what is to be licensed. If a proposed regulatory system is to stop short of

requiring the licensing of all manufacturers engaged in the production of any device which transmits or records wire or oral communications or facilitates such transmission or recordation, then its drafters must cope with the same definitional problem existent in Section 2512. Even under an all-inclusive regulatory system, once the licensed manufacturer sells an innocuous device such as an automatic telephone answerer there is no way to preclude the purchaser from using that device for wiretapping. Further, to the extent that a manufacturer is presently willing to violate the felony provisions of Section 2512, it seems unlikely that a licensing requirement would have any impact. It is our belief that the additional level of bureaucracy inherent in such a regulatory system would be justifiable only as a last resort, and then only if a highly effective system can be developed.

It appears that the better method of curbing the availability of electronic surveillance devices is by increasing the risk involved in their use. We believe that this could be accomplished through the amendment of Section 2511 to create a misdemeanor violation and a strict liability civil penalty, suggestions which were discussed at some length earlier.

2. Amendment of Section 2513: While the Murdock standard of willfulness may be appropriate for a felony prosecution, there appears to be no justification for requiring such a heavy burden of proof in a forfeiture proceeding. We believe that proscribed devices should be subject to forfeiture solely on the objective basis of their nature or the nature of the advertising. Additionally, a strict liability civil penalty would be of valuable assistance in enforcing the prohibitions of Section 2512.

3. Export of Interception Devices: Manufacturers of surveillance devices complain that there should be a licensing procedure whereby they could be exempted from the provisions of Section 2512 for the purpose of making sales to foreign governments. At present, the only way in which such a sale could be effected would be if the transaction is brought within the exceptions contained in Section 2512(2)(a) or (b). The exception in 2512(2)(a) seems inapplicable as there would appear to be no way in which a common carrier could enter into a contract for the sale of proscribed devices to a foreign government pursuant to the normal course of its business activities. Similarly, such transactions would appear to be outside the normal business activities of state and local law enforcement agencies, 18 U.S.C. 2512(2)(b). However, some federal law enforcement agencies routinely, as a normal part

of their activities, cooperate with foreign police departments in an effort to combat crimes which have an international connection; for example, hijacking, the international flow of narcotics, and international terrorism. If, pursuant to those normal, cooperative law enforcement efforts, a U. S. investigative agency enters into a contract between a foreign police department and a U. S. producer of proscribed devices for the sale and delivery of such devices to the foreign police department, such transaction would appear to fall within the exception of Section 2512(2)(b). However, this is not an area subject to blanket prior determinations. Each proposed sale and export of proscribed devices to a foreign government would have to be individually evaluated to determine whether the transaction is, in fact, pursuant to the normal course of activities of the participating U. S. Government agency, and thus legal under Section 2512.

It is clear that the existing system for export of surveillance devices is cumbersome, and federal investigative agencies have shown a reluctance to become involved in the process. Accordingly, in the event that at some time in the future the need is exhibited by a significant number of foreign police departments for surveillance devices produced only within the United States, we would then favor serious consideration of an export licensing exception to Section 2512. However, at present we do not view the legitimate demand for such devices to be sufficient to merit the legislation. Absent a genuine need, the enactment of such legislation would appear inadvisable as it might encourage more businesses to begin producing such devices.

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

BEFORE: HONORABLE ROBERT H. SCHNACKE, JUDGE

UNITED STATE OF AMERICA, Plaintiff

-vs-

JOHN CHRISTMAN, Defendant

NO. CR 74-123 RHS

REPORTER'S TRANSCRIPT

TUESDAY, MAY 7, 1974

Reported by:

CAROL JAMES, C.S.R.

KENNETH COMBS, C.S.R.

APPEARANCES:

For the Plaintiff:

JAMES L. BROWNING, JR.

United States Attorney

BY: JAMES DAFFER

Assistant United States Attorney

450 Golden Gate

San Francisco, California 94102

For the Defendant:

GREGORY S. STOUT, Esquire

One California Street

San Francisco, California

MAY 7, 1974

(PROCEEDINGS IN COURTROOM, JURY ABSENT)

THE COURT: The first thing we must consider here is that this is a criminal prosecution. The statute is to be applied only in the event that its language requires a finding of guilt under the circumstances disclosed by the evidence. If any reasonable interpretation of any of the exceptions of the statute would apply to the conduct described by the government's case, it would follow that we must accept that exception as intending to negate criminal activity under the circumstances described.

The Fifth Circuit, in *Simpson against Simpson*, was involved with almost exactly the circumstance I indicated earlier, of the husband listening in on his wife's conversation. (In it is made the charming comment that the conversations overheard were mildly compromising in that "while the wife was resisting, she was not doing so in a firm and final fashion." The Court there indicated that Congress had considered that kind of interception. The reference to that kind of interception is in the testimony of the witness before Congress who also referred to business sur-

veillance of business personnel and the comment of the First Circuit was, at page 809, "These statements suggest Congressional awareness that private individuals were using electronic surveillance within their own homes. However, they do not support the proposition that Congress was concerned that such activities took place."

Now, it seems to me that surveillance techniques within a home are very similar to surveillance techniques within the family of a business organization. Congress was aware that those things were happening, and yet it would appear from some of the exceptions provided by Congress that they were excluding prosecution of that kind of surveillance.

We find two areas where that comes up. The first is the extension telephone exception in 2510(5)(a) which makes it plain that merely listening in on an extension telephone is not the kind of interception Congress is prohibiting.

The evidence in this case—at least the testimony of the installer—was that an extension telephone had been installed, and it was through that extension telephone that this interception took place.

Now, whether there was an instrument there or not, the equipment and facility had been installed by the carrier in the ordinary course of its business, which was to protect Macy's from improper activities by its employees. I believe that is a rational reading of that exception, and the defendant is entitled to have it read rationally in his favor.

EXCERPT FROM ELECTRONIC SURVEILLANCE
CRITICS QUESTIONNAIRE

12. Is the Federal law effective in its prohibition of manufacturing, distribution, possession and advertising of wire or oral communication interception devices for purposes not related to the needs of a communications common carrier or of law enforcement? Should manufacturers of such equipment be subject to licensing? Do you have any other suggestions for stemming proliferation of this equipment? There have been a number of reports in the media of illegal wiretapping by local police (Houston, Williamsport [PA], Cedar Rapids [IA], NYC). Do you have any views as to the competency of the FBI to investigate such cases? Is there an alternative?

13. Is the exception granted to communications common carriers to intercept communications insofar as necessary to the protection of the rights or property of the carriers of such communications too broad? Should the statute explicitly proscribe interception of telephone communications of employees in an office by the employers? What of companies which conduct most of their business by telephone, such as airlines reservations? Is there any expectation of privacy in communications by an employee on a business telephone? If so how should that expectation be defined?

ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISIONDepartment of Justice
Washington 20530

May 20, 1975

General Kenneth J. Hodson
Executive Director
National Commission for the Review of
Federal and State Laws Relating to
Wiretapping and Electronic Surveillance
1875 Connecticut Avenue, N. W.
Washington, D. C.

Dear General Hodson:

Your letter to the Attorney General, dated April 17, 1975, has been referred to this Division for attention.

In that letter you indicated that one area of particular interest to the Commission concerns the effectiveness of Title 18, United States Code, Sections 2511 and 2512 in reducing and controlling illegal electronic surveillance. You posed eleven specific questions designed to elicit information relevant to the manner in which those statutes are administered by this Department. I will respond to your questions individually.

1. How many Department of Justice attorneys in Washington have direct responsibilities for matters dealing with violations of 18 U.S.C. 2511-12? Primary responsibility for the administration of these statutes is vested in a unit of the General Crimes Section of this Division staffed by four attorneys. These attorneys play a major role in the formulation of Departmental policies and positions under Sections 2511 and 2512, and provide guidance to Assistant United States Attorneys in the handling of prosecutions brought under these sections.

2. Approximately how much of their time is devoted to these matters? As a group, these four attorneys devote approximately 40% of their time to matters related to the enforcement of Sections 2511 and 2512.

3. Do written guidelines exist for administering illegal electronic surveillance complaints and prosecutions? If so please submit. Yes, such written guidelines are contained in Department of Justice Memorandum Number 613 and 613, Supplement Number 1. Copies of those memoranda are attached. As with any prosecutive policy, the guidelines reflected in attached memoranda specify areas of primary prosecutive interest as well as areas of relatively secondary interest. Any widespread dissemination of these memoranda might have the deleterious effect of fostering in some persons the erroneous view that certain types of violations can be committed with impunity. Accordingly, it is requested that the Departmental memoranda be used on a need to know basis and that they not be made public exhibits.

4. What is the Justice Department policy towards prosecution of illegal eavesdropping in domestic relations cases? Does the Department have a different policy towards prosecution of other types of illegal electronic surveillance? Has your policy been altered by Simpson vs. Simpson, 490 F.2d 803 (CA 5 1974)? The Department's overall prosecutive policy under Section 2511 has been to focus primarily on persons who engage in or procure illegal electronic surveillance as part of the practice of their profession or incident to their business activities. This includes private investigators, attorneys, law enforcement officials, and business executives. Less emphasis is placed on the prosecution of persons who, in the course of a transitory situation such as a marital dispute, endeavor to intercept communications on their own, without the assistance of a professional wiretapper or eavesdropper. This does not mean that the Department has never prosecuted one spouse for his or her individual undertaking to intercept the communications of the other spouse. It is simply that such prosecutions are not a major thrust of the Department's enforcement program. Similarly, where one spouse hires a private investigator to conduct electronic surveillance on the other spouse, the Department will, when necessary, forego the prosecution of the offending spouse in favor of using his or her immunized testimony to build a prosecutable case against the private investigator.

The Department's policy in this regard has its underpinning not only in the efficient allocation of limited resources but also in the standard of willfulness embodied in Section 2511. The legislative history of that section defines "willful" by citing United States v. Murdock, 290 U.S. 389 (1933). Senate

Report No. 1097, Omnibus Crime Control and Safe Streets Act of 1967 [later changed to 1968], April 29, 1968, page 93. That case defines willful to mean an act done with a bad purpose or evil intent. Further, the court in Murdock cited approvingly decisions which defined willful in terms of "a thing done without ground for believing it lawful" and "conduct marked by careless disregard whether or not one has the right so to act." In a prosecution against a spouse for domestic relations electronic surveillance, it is often difficult or impossible for the Government to sustain its burden of proof under this definition of willful. This is especially true in the face of the frequently repeated view that it is legally permissible for a spouse to engage in electronic surveillance within his own home or on his own telephone.

Our prosecutive policy as outlined above has not been altered by the Fifth Circuit decision in Simpson v. Simpson. In our view the Simpson decision was incorrectly decided. In that case, the Fifth Circuit held that the civil remedies portion of the federal electronic surveillance statute (18 U.S.C. 2520) does not allow recovery by a wife in a suit against her husband for wiretapping by the husband of the phone in the couple's marital home. Unfortunately, the decision inferentially and in dicta indicates that such interspousal wiretapping is not a crime.

The court in Simpson conceded that the clear wording of the statute appears to proscribe such wiretapping. However, in deference to the traditional interspousal immunity from tort actions, the court undertook a search of the legislative history of the statute to determine if Congress had specifically expressed a desire to apply the statute to interspousal wiretapping. Finding no controlling expressions of legislative intent, the court hesitantly reached its decision, stating in so doing that "we are not without doubts about our decision" and "our decision is, of course, limited to the specific facts of this case." Simpson v. Simpson, 490 F.2d 803, 810 (CA 5, 1974); cert den 43 U.S.L.W. 3239 (U.S., Oct. 22, 1974).

The relevant legislative history uncovered by the court is set forth in a footnote to the decision. Unfortunately, the court

did not locate portions of the legislative history which indicate explicitly that the proscriptions of Section 2511 are designed particularly for applicability to electronic surveillance conducted in domestic relations and industrial espionage situations. In view of such expressions of Congressional intent, the Department has not altered its prosecutive policy to conform with Simpson. We have on several occasions since the Simpson decision prosecuted a spouse for electronic surveillance conducted within the marital home. However, no additional law has been developed on this issue as the defendants have not raised the Simpson issue.

The main difficulty encountered as a result of Simpson has been its derivative effect on the element of willfulness. In prosecutions brought against attorneys and private investigators for involvement in electronic surveillance emanating from marital disputes, the Government is occasionally encountering the argument that the defendant relied on Simpson in advising a client to wiretap or in carrying out the wiretap for the client, and thus did not willfully violate Section 2511. This argument can cause serious problems for the prosecution in view of the Murdock standard of willfulness contained in the statute and the fact that this argument is generally raised in the form of a motion for judgment of acquittal, thus allowing the prosecution no appeal from an adverse decision by a trial judge.

5. How many prosecutions have been initiated under 2511(1)(a)? What enforcement problems, if any, exist in this section? The statistics maintained by this Department on Section 2511 are not subdivided to show the specific number of prosecutions brought under each subsection. Generally, where there has been an interception in violation of Section 2511(1)(a) or (1)(b) there are also accompanying violations of Section 2511(c) and (d) - i.e., knowing disclosure and use of the intercepted information. Accordingly, even though a defendant may be indicted on three different counts involving violations of Section 2511(1)(a), (c), and (d), the indictment is reflected in our statistics as one case brought under Section 2511.

Without resorting to specific statistics, it is possible to say that Section 2511(1)(a) has been used frequently. All prosecutions for the interception of wire communications are brought under 2511(1)(a). The enforcement and prosecutive problems encountered in such cases, as in all cases brought under 2511, can be placed into five general categories: (1) The difficulty

in establishing willfulness, discussed above. (2) The potential problem posed by the reasoning of the Simpson decision and the existing problem encountered in its derivative effect on proof of willfulness. (3) The fact that illegal electronic surveillance is a crime which often produces noncomplaining victims. To the extent that the surveillance goes undetected, its victims are unaware that they have been the subject of a crime. Moreover, in instances of domestic relations electronic surveillance (by far the most common type of electronic surveillance) the victims frequently choose not to lodge a complaint for fear that the ensuing investigation and trial will focus attention on their own indiscretions. Domestic relations surveillance violations are often reported by a disinterested party, such as a telephone repairman, and the ensuing investigation finds the victims totally uncooperative. As an example, in a recent case a victim of an illegal intercept apprised this Department in no uncertain terms that he would do everything possible to thwart a prosecution. He appealed for the discontinuation of our investigation by stating that a prosecution would do far greater violence to his privacy than did the illegal intercept. (4) The fact of judicial nullification. On several occasions United States District Court judges have been openly defiant of Government efforts to prosecute Section 2511 violations. More common, however, are expressions of judicial distaste for prosecutions emanating from marital disputes, an attitude which sometimes appears to inure to the benefit of the defense. Doubts have been expressed as to whether U. S. District Court is the appropriate forum, and a felony prosecution the appropriate medium, for disposition of domestic relations wire-tapping and eavesdropping cases. (5) The fact of jury nullification. Again, this problem is particularly critical in prosecutions resulting from marital disputes. One strongly suspects that in such prosecutions the Government is sometimes viewed by jurors as the defender of persons caught in immoral conduct. In some cases, there may be a tendency to consider the results of the given instance of electronic surveillance as vindicating its use.

In posing your question concerning enforcement problems under Section 2511(1)(a), we presume that you are, at least in part, referring to the question of the constitutionality of that subsection as applied to eavesdropping violations (i.e., the interception of oral communications). The existence of the constitutional issue is thoroughly documented and analyzed in the legislative history of the statute. See Senate Report No. 1097, supra, page 92; Hearings before the Subcommittee on Administrative

Practice and Procedure of the Senate Judiciary Committee, 90th Cong., 1st Sess., on the Right of Privacy Act of 1967, Part II, p. 441 et seq. We are generally able to avoid the constitutional question by prosecuting eavesdropping violations under one of the delineated categories of Section 2511(1)(b) which has an established connection to interstate commerce. Our experience to date indicates that only rarely are all of the categories of 2511(1)(b) inapplicable to a given act of eavesdropping, and thus resort to 2511(1)(a) necessary. However, the Department is presently involved in the prosecution of such a case. Predictably, the case is now on appeal to the United States Court of Appeals for the Fourth Circuit with the key issue being the constitutionality of the blanket eavesdropping prohibition contained in Section 2511(1)(a). If the court's decision reaches the constitutional issue, it will represent the first appellate determination in this regard.

6. Do you have difficulty in interpreting 2511(2)(d), specifically the words ". . . or for the purpose of committing any other injurious act"? Yes, that final phrase of Section 2511(2)(d) does create problems of interpretation. The remainder of subsection (2)(d) appears clear in meaning. The subsection permits persons not acting under color of law to intercept a communication where one of the parties to the communication has given prior consent, unless the communication is intercepted for the purpose of committing a criminal or tortious act "or for the purpose of committing any other injurious act."

Section 2511(2)(d) was added to the statute as a floor amendment introduced during Senate debate by Senator Hart. As such, there is scant legislative history to explain the intended meaning of "other injurious acts." See 114 Congressional Record 14694 (May 23, 1968); Senate Report No. 1097, supra, additional views of Mr. Hart, p. 175. That legislative history indicates that the overall intent behind 2511(2)(d) is to make the one party consent exception available only for "private persons who act in a defensive fashion." 114 Congressional Record 14694. One party consent interceptions are prohibited when the consenting party "acts in any way with an intent to injure the other party to the conversation..." 114 Congressional Record 14694. The only example provided of a non-criminal or tortious intent to injure is the secret, one party consent recording of a conversation for the purpose of "publicly embarrassing" the nonconsenting party. 114 Congressional Record 14694. Some further light is shed on the meaning of the statutory provision by the delineation of two types of one party consent

interceptions which are not prohibited: (1) a recording made of "information of criminal activity by the other party with the purpose of taking such information to the police"; and (2) a recording made out of a "legitimate desire to protect himself and his own conversations from later distortion . . . by the other party." 114 Congressional Record 14694.

This Department has never sought to base a prosecution on the instant statutory provision, i.e., a one party consent recording made for the purpose of committing a noncriminal or tortious injurious act. However, there are certainly some equitable wrongs for which no criminal or tort remedies are available. It remains possible that a suitable flagrant situation might arise where the Department would institute a criminal prosecution based on the instant statutory provision. It appears unlikely, however, that the provision as presently drafted will play a significant role in the Department's enforcement program.

7. What criteria does the Justice Department use in determining if a device is "primarily useful for the purpose of the surreptitious interception of wire or oral communication"? Have you had difficulty deciding the nature of some devices? If so give examples. Has Justice Department policy on interpretation of 2512 been altered by U. S. vs. James A. Six; USDC ND Indiana 1970? In determining which devices are primarily useful for the surreptitious interception of communications, we rely heavily on the examples set forth in the Senate Report prepared on the bill. Senate Report No. 1097, supra, p. 95. It appears that the proscribed devices delineated in that legislative history are of two basic types: (1) disguised listening devices, and (2) devices designed to intercept communications occurring elsewhere than the location of the interceptor. As long as the statute is strictly applied to those two types of devices, there appears to be a reasonable basis for determining whether a given device is primarily useful for the surreptitious interception of communications. However, the test established by the statute is a factual test — i.e., ~~whether~~ the attributes of a device give predominance to the surreptitious character of its use — and, as with any factual determination, there will always be some close calls which are difficult to make.

It is important to realize the limitations of Section 2512. The legislative history makes it clear that it is designed to proscribe "a relatively narrow category of devices whose principal use is likely to be for wiretapping or eavesdropping." Senate Report No. 1097, supra, p. 95. As applied to such a narrow category of devices, the statute appears relatively effective. However, the statute is not designed to and does not have the capability of preventing the possession and distribution of all electronic devices which may prove of assistance to wiretappers and eavesdroppers.

The Department's interpretation of Section 2512 has not been altered by the U. S. District Court decision in United States v. James A. Six (N. D. Indiana, 1970). The Government's prosecution in that case terminated with a finding of not guilty by the trial judge after a bench trial. In that situation no appeal was possible. The judge based his finding of not guilty on his conclusion of law that the word "willfully" as used in Section 2512 requires that the defendant's possession of a proscribed device must have been with knowledge that the possession was prohibited by law and "with the purpose of violating the law." No case law or legislative history was cited in support of this ruling. It is difficult to determine exactly what the judge meant by the phrase "with the purpose of violating the law." However, if the intended meaning was that the defendant must possess the device with the purpose of using it in violation of 18 U.S.C. 2511, such position is clearly rebutted in the Court of Appeals decision in United States v. Bast, 495 F.2d 138 (CA D.C., 1974). The decision in U. S. v. Six is unpublished. In our view the judge's definition of "willfully" — even accepting the more moderate of its possible interpretations, i.e., that there must be specific intent to violate Section 2512 — is without any legal foundation. We know of no other case under 18 U.S.C. 2512 in which a court has adopted such a definition.

8. With reference to section 2512(2)(a), have any standards been devised to determine what is the ". . . normal course of the communications common carrier's business" (for this purpose, assume that in 1971 an individual representing the International Telephone and Telegraph Corporation possessed and transported to a foreign nation devices prohibited by 2512)? No such standards have been devised. The question of what activities are in the normal course of a communication common carrier's business calls for a factual judgment which is not subject to a blanket prior

determination. Each instance must be judged on its own unique facts. However, to pursue the subject matter of your question a bit further, it is possible to draw some general conclusions. We do know from Section 2511(2)(a)(i) that it is legally permissible for an officer, employee, or agent of a communications common carrier to intercept communications under the conditions delineated in that subsection. The exception contained in Section 2512(2)(a) provides a concomitant right for communication common carrier personnel to possess proscribed interception devices. Such a statutory exception appears necessary to give full meaning and effect to the carrier's right to intercept. Conversely, the carrier's right to possess such proscribed devices appears limited to that possession necessary to carry out legitimate interception activities authorized by 2511(2)(a)(i). Accordingly, to be possessed in the normal course of the carrier's business, the proscribed device must be possessed as a normal and reasonable incident to the carrier's powers under 2511(2)(a)(i).

The legitimacy of a common carrier transporting a proscribed device from the United States to a foreign country would have to be gauged analogously. If the common carrier has facilities in a foreign country, its transport of devices to that country for its own use would appear to be in the normal course of business so long as the intended use is compatible with 2511(2)(a)(i) or with the law on common carrier intercepts in the foreign country.

9. How do you interpret the portion of 2512(2)(b) which provides an exception for an "officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State or a political subdivision thereof. . ." (i.e., can a police officer or department purchase and/or possess prohibited devices in a State that does not have legislation authorizing court-authorized wiretapping)? As indicated in the answer to the previous question, we hesitate to make blanket prior determinations concerning what constitutes the normal course of activities of a law enforcement agency. However, it is possible to draw some conclusions on the specific situation posed in your question. As a general statement, as long as proscribed interception devices are used by governmental police agencies for a legal law enforcement purpose, the exception contained in Section 2512(2)(b) is applicable and the prohibitions of Section 2512(1) remain inactive. Once the equipment is used either illegally or for other than a law enforcement purpose,

resort to the statutory exception is lost, and the provisions of Section 2512(1) are activated, making possession illegal.

If a state has no authorizing statute for the purpose of meeting the requirement of 18 U.S.C. 2516(2), it cannot be in the normal course of activities of state and local police departments in that state to intercept communications without at least one party consent. Accordingly, it cannot be in the normal course of their activities to possess equipment primarily useful for the nonconsensual interception of communications. However, one party consensual interceptions are permissible under the federal electronic surveillance statute if intercepted "under color of law," 18 U.S.C. 2511(2)(c). So long as such intercepts are permitted under state law, the state and local police may legally engage in one party consent intercepts. Since such intercepts would then be both legal and for a law enforcement purpose, the equipment used is exempted from the prohibitions of Section 2512(1).

Accordingly, even though the state is a "non-authorization state" it would be legal for police departments to possess those devices proscribed by Section 2512(1) which are designed for one party consent interceptions. It would not, however, be legal for them to possess devices designed for nonconsensual interceptions.

10. Under what circumstances, if any, could a manufacturer/distributor sell prohibited devices to a foreign government? The only way in which such a sale could be effected would be if the transaction is brought within the exceptions contained in Section 2512(2)(a) or (b). The exception in 2512(2)(a) seems inapplicable as there would appear to be no way in which a common carrier could enter into a contract for the sale of proscribed devices to a foreign government pursuant to the normal course of its business activities. Similarly, such transactions would appear to be outside the normal business activities of state and local law enforcement agencies, 18 U.S.C. 2512(2)(b). However, some federal law enforcement agencies routinely, as a normal part of their activities, cooperate with foreign police departments in an effort to combat crimes which have an international connection; for example, hijacking, the international flow of narcotics, and international terrorism. If, pursuant to those normal, cooperative law enforcement efforts, a U. S. investigative agency enters into a contract between a foreign police department and a U. S. producer of proscribed devices for the sale and delivery of such devices to the foreign police department, such transaction would appear to fall within the exception of Section 2512(2)(b). However, this is not


an area subject to blanket prior determinations. Each proposed sale and export of proscribed devices to a foreign government must be individually evaluated to determine whether the transaction is, in fact, pursuant to the normal course of activities of the participating U. S. Government agency, and thus legal under Section 2512.

11. Under what circumstances, if any, could a manufacturer/distributor display or demonstrate prohibited devices to a potential client? Under the terms of Section 2512, it is not legal for retailers or distributors to purchase proscribed devices for resale. Sales must be made directly from the manufacturer to the authorized purchaser. Further, except for the situation discussed in the answer to question 10 above, the only authorized purchasers of devices proscribed by Section 2512 are communications common carriers, governmental law enforcement agencies, and officers, agents, and employees thereof. Demonstration of prohibited devices to these clients can be accomplished under the same conditions that a sale can be accomplished. In other words, the authorized purchaser may, in the regular course of its activities, enter into a contract with a manufacturer for the construction of sample devices to be demonstrated to that prospective purchaser.

At the close of your letter, you asked to be advised of the status of the eavesdropping complaint involving one Donald L. Uffinger which you referred to this Department in October, 1974. You indicated in your letter that if the matter has been disposed of it might provide the Commission with an opportunity to examine a case from its inception. Please be advised that the complaint is still under investigation. Accordingly, no further comment on the matter by this Department is appropriate at this time.

If we can be of any further assistance to you, please feel free to contact us.

Sincerely,


JOHN C. KEENEY
Acting Assistant Attorney General

EXTRACT

DEPARTMENT OF JUSTICE
WASHINGTON, D.C. 20530

July 7, 1971

MEMO NO. 613
SUPPLEMENT No. 1

TO ALL UNITED STATES ATTORNEYS

SUBJECT: *Interception of Communications*

To provide a better understanding of the Act and insure uniformity in construction, we discuss below a number of common misconceptions concerning these provisions of law. The first is the question of scope of authorized activities under the exceptions in 18 U.S.C. 2512. The exceptions do not permit advertising and do not permit transactions directly with foreign governments. The exceptions authorize only manufacture, distribution, and possession. Thus, a dealer may not advertise prohibited devices even though he circularizes only authorized purchasers. On the other hand, he may advise such purchasers that his firm is generally skilled in the production of electronic devices and respond to specific inquiries with information requested on prohibited devices. In addition, a dealer may not maintain an inventory of assembled prohibited devices in anticipation of obtaining a contract with an excepted buyer, nor does a particular supplier's contract with an excepted purchaser legitimize another supplier's transactions with the prime contractor.

As to foreign governments and others for that matter, if an excepted buyer in the normal course of its activities becomes a party to a sale to a third entity, we view the exception as applicable to the transaction as a whole.

Another misconception as to activities allowed by Title III is the belief that a telephone subscriber may intercept communications on his own service without violating the law. The fact that a tap is put on the subscriber's own phone in his own house or place of business is an irrelevant matter under 18 U.S.C. 2511. The exception pertains to parties, not to subscribers. Implied consent may exist if notice is given. And even if the interception is not in violation of section 2511, the device used to make the interception may still be prohibited by section 2512.

It should also be noted that anyone who sells any device for use in interception falls within 18 U.S.C. 2 as an aider and abettor and is equally guilty with the principal for the latter's violation of 18 U.S.C. 2511 by means of the device provided.

Finally, problems may arise regarding illegal interception by local law enforcement agencies. Local authorities should be made to clearly understand that we cannot condone violations even if done for a worthy purpose. In light of 18 U.S.C. 2516(2) local authorities have no excuse for illegal interception activities.

A concerted effort should now be made by United States Attorneys to refer complaints to local authorities in those states which have reasonably adequate statutes, absent special circumstances warranting Federal action. See Memo No. 613, page 12. Those states having reasonably adequate statutes prohibiting both the interception of wire and oral communications are as follows: Alaska, Arizona, California, Colorado, Florida, Georgia, Hawaii, Illinois, Massachusetts, Minnesota, New Hampshire, New Jersey, New York, and Oregon. States having adequate statutes only against the interception of wire communications are: Idaho, Kentucky, Montana, Nebraska, North Dakota, Ohio, Oklahoma, Pennsylvania, and Wyoming.

United States Attorneys in those states lacking adequate laws should encourage adoption of adequate local prohibitions, noting that it is in those states that local offenders will be most tempted to intercept without authority. The Department will continue to monitor state programs for the adoption of effective

laws and the institution of effective enforcement programs. When it becomes plain in a particular state that the authorities are indifferent to such invasions of the privacy of their citizens, as demonstrated by their failure either to enact effective statutes or to effectively enforce them, we should cease to endeavor to thrust Federal policy upon them and limit prosecution to those cases having, again, a substantial Federal interest or involving out-of-state residents.

Investigative-prosecutive activities under Title III will continue to be coordinated by a special unit within the General Crimes Section of the Criminal Division (Extension 2346).

(Signed)
WILL WILSON
Assistant Attorney General
Criminal Division

EXHIBIT NO. 16
Simpson v. Simpson, 490 F.2d 803 (5th Cir., 1974)
14 CrI 2495 (3/27/74)

HUSBAND WIRETAPPING WIFE DOESN'T
VIOLATE '68 CRIME CONTROL ACT

Thorough review of scanty legislative history convinces CA 5 that there was no criminal violation or compensable tort.

The difference between Congressional awareness and congressional concerns dooms the efforts of a divorced wife to get civil damages under Title III of the 1968 Omnibus Crime Control Act for her ex-husband's wiretapping of her phone conversations within the marital home. The Fifth Circuit's exhaustive review of what little legislative history there is shows that while Congress expressed awareness of the problem of detective-assisted marital bugging and tapping, it didn't clearly express the kind of concern that would justify extending federal legislation into the field of domestic relations and the privacy of marital domiciles.

Although on its face Title III's broad language might reach such snooping by spouses, it will take a lot more to convince the Fifth Circuit that anything but a restrictive interpretation of this language is justified. One reason is avoiding the unwarranted extension of federal power into new areas where congressional intent is not clear. The other is that this is largely criminal legislation designed to regulate abuses in the criminal justice field, and includes parallel criminal provisions that would expose jealous husbands and wives to harsh jail terms for activities which may be designed to protect their marriages. Thus the plaintiff, who also invoked right-of-privacy and sexual equality arguments that the court thinks irrelevant, fails to collect under 18 U.S.C. 2520. (*Simpson v. Simpson*, 3/8/74)

Digest of Opinion: [Text] The issue presented on this appeal is the scope of the wire interception provisions of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C.A. Secs. 2510—2520. Is the interception by a husband using electronic equipment of the conversation of his wife with a third party over the telephone in the marital home included in the statutory proscription? The context in which we must address this issue is a suit by the wife for civil damages against the husband, pursuant to Section 2520. The district court answered in the negative and we affirm, although the language and legislative history of the Act leaves the question in considerable doubt. [*End Text*]

The conversations the husband obtained were mildly compromising or ambiguous as to actual adultery, but when he played them for the wife's lawyer, the lawyer advised, and the wife agreed to, an uncontested divorce.

[*Text*] After the divorce, appellant brought this action. Failing below, she has appealed, arguing before this court that her claim is bolstered by constitutional protections of privacy and emerging concepts of women's rights. We take a more pedestrian view

of the case, and are of the opinion that it involves nothing more nor less than statutory construction. If Congress intended to extend such a remedy to persons in her position, appellant prevails; if it did not, she fails. This being the case, we turn to the statute and its history. * * *

The naked language of Title III, by virtue of its inclusiveness, reaches this case. However, we are of the opinion that Congress did not intend such a far-reaching result, one extending into areas normally left to states, those of the marital home and domestic conflicts. We reach this decision because Congress has not, in the statute, committee reports, legislative hearings, or reported debates indicated either its positive intent to reach so far or an awareness that it might be doing so. Given the novelty of a federal remedy for persons aggrieved by the personal acts of their spouses within the marital home, and given the severity of the remedy seemingly provided by Title III, we seek such indications of congressional intent and awareness before extending Title III to this case.

Our independent search of legislative materials has been long, exhaustive, and inconclusive. * * *

An initial observation about Title III is that it is a part of a crime control act * * *

Be this as it may, Title III also was intended to protect individuals against invasions of their privacy by sophisticated surveillance devices. (*End Text*)

The Senate's report expresses awareness of the problem that no one is assured privacy anymore and that words spoken as to private personal and marital concerns can be intercepted and used against the speaker. It adds that to assure privacy of wire communications, Title III prohibits all tapping and bugging by non-police persons.

[*Text*] For our purposes it must be pointed out that we have herein quoted virtually every phrase of the report's text dealing with private surveillance—amounting to less than one of the ten pages about Title III, the balance concerning electronic surveillance by law enforcement officials. Not only does the report, like the act, focus on crime control, but it also contains no clear indication that Congress intended to intrude into the marital relation within the marital home. We thus have considered it necessary to consult the extensive legislative hearings on the subject, the better to gauge Congress's intent and awareness.

The impression left by these hearings is similar to that produced by the report—the focus was official use of surveillance devices, with little explication of how far the private prohibition should extend. [*End Text*]

The only relevant passages we have found in over five years of hearings concern testimony by three private detectives and a district attorney [set forth in the court's footnotes] indicating that the practice of bugging in marital disputes is common, that detectives tend to restrict it to supplying bugging equipment and advice to husband or wives wishing to tap within their own homes, and that private detectives sometimes justify the practice by saying that in their experience, whenever the truth is out there is a far better chance, statistically, of reconciliation.

[*Text*] These statements suggest congressional awareness that private individuals were using electronic surveillance techniques within their own homes. However, they do not support the proposition that Congress was concerned that such activities took place.

Given this inconclusive legislative history, we think two other factors are important. First, it is clear that Congress did not intend to prohibit a person from intercepting a family member's telephone conversations by use of an extension phone in the family home—subsection (5)(a)(i) of section 2510 directly covers this point. If there is a convincing distinction between this clearly acceptable overhear and the overhear accomplished by appellee, we fail to see it. In fact, we think the (5)(a)(i) exemption is indicative of Congress's intention to abjure * * * deciding a very intimate question of familial relations, that of the extent

of privacy family members may expect within the home vis-a-vis each other.

Second, we note that not only does Title III have the primary goal of controlling crime, but that it also prescribes criminal sanctions for its violators. That is, if appellant prevails here then appellee is subject to severe criminal penalties, assuming of course that the prosecution could meet the higher standards of proof required for criminal convictions. We thus are bound by the principle that criminal statutes must be strictly construed, to avoid ensnaring behavior that is not clearly proscribed. See *Kordel v. United States*, 1948, 335 U.S. 345, 349, 69 S.Ct. 106, 109, 93 L.Ed. 52, 56. We consider this basic due process principle to be of considerable importance in this case, in light of our own inability to determine from the statute and its legislative history whether one is prohibited from tapping one's spouse's conversations within one's own home.

As should be obvious from the foregoing, we are not without doubts about our decision. However, we have concluded that the statute is not sufficiently definite and specific to create a federal cause of action for the redress of appellant's grievances against her former husband. Our decision is, of course, limited to the specific facts of this case. No public official is involved, nor is any private person other than appellee, and the locus in quo does not extend beyond the marital home of the parties.

Affirmed. [*End Text*].—Bell, J.
(*Simpson v. Simpson*; CA 5, 3/8/74)

EXHIBIT NO. 17

Statistics of Complaints Received and Prosecutions Pursued under the Criminal Provisions of Title III, Omnibus Crime Control and Safe Streets Act of 1968

It is difficult to determine accurately the magnitude of illegal electronic surveillance. To the extent that the surveillance goes undetected, its victims are unaware that they have been the subject of a crime and no complaint is made. Further, in instances of domestic relations electronic surveillance, victims often choose not to lodge a complaint for fear that the ensuing investigation and trial will focus attention on their own indiscretions. On the other hand, many complaints are made by persons acting on mere suspicion and without any object basis for their belief. This is reflected in the fact that less than 2% of the wire-tapping complaints investigated by AT&T affiliates produce any evidence of a possible tampering with the telephone line.

The FBI, in conjunction with the U.S. Attorneys' offices, seeks to weed out the clearly spurious and unfounded allegations and to confine their investigative efforts to complaints which appear at the outset to have some factual support. The statistics on the resulting category of "cases received for investigation" are contained in the first table which follows. However, in reviewing those statistics it should be kept in mind that a significant percentage of the cases received for investigation ultimately prove to constitute unfounded complaints.

The statistics which follow have been organized into five subject areas:

1. Complaints received by the FBI
2. Cases filed (indictments and informations)
3. Cases terminated
4. Analysis of cases terminated
5. Disposition of appeals

Complaints Received by the FBI

The statistics set forth below are compiled by the FBI and represent what they classify as "cases received for investigation." This term, defined generally, means all complaints which appear at the outset to state a *prima facie* violation of the

Federal criminal statute in question. The statistics are compiled for the broad classification of interception of communications violations, which includes 18 U.S.C. 2511 and 2512 and 47 U.S.C. 605. Separate statistics are not maintained for the individual statutes. A case is categorized under the subject matter of the initial complaint. Therefore, if an interception of communications investigation evolves from an investigation begun in another statutory area, that investigation would not be reflected in these statistics.

The statistics of complaints received by the FBI in Fiscal Year 1975 are based on data through the first ten months of the fiscal

year.

<i>Fiscal Year</i>	<i>Complaints Received by FBI</i>
1969	433
1970	541
1971	521
1972	541
1973	569
1974	701
1975	688
TOTAL	3,994

CASES FILED (INDICTMENTS AND INFORMATIONS)
UNDER THE INTERCEPTION OF COMMUNICATIONS STATUTES

The statistics cited below exclude superseding indictments and informations. This was done to avoid having some cases reflected in the statistics two or more times.

The statistics for Fiscal Year 1975 are based on data through the first nine months of the fiscal year.

Fiscal Year	18 U.S.C. 2511		18 U.S.C. 2512		47 U.S.C. 605		Total	
	Cases	Defendants	Cases	Defendants	Cases	Defendants	Cases	Defendants
1969.....	3	3	1	1	3	4	7	8
1970.....	3	3	3	4	3	4	9	11
1971.....	8	12	2	2	—	—	10	14
1972.....	15	21	6	7	2	2	23	30
1973.....	19	33	3	4	1	1	23	38
1974.....	19	24	2	3	2	3	23	30
1975.....	14	22	2	2	3	3	19	27
Total	81	118	19	23	14	17	114	158

INTERCEPTION OF COMMUNICATIONS
CASES TERMINATED

The statistics below exclude all nonfinal terminations such as dismissal of charges followed by the filing of a superseding indictment or information in the same case. This was done to avoid having some cases reflected in the statistics two or more times.

The statistics for Fiscal Year 1975 are based on data through the first nine months of the fiscal year.

Fiscal Year	18 U.S.C. 2511		18 U.S.C. 2512		47 U.S.C. 605		Total	
	Cases	Defendants	Cases	Defendants	Cases	Defendants	Cases	Defendants
1969.....	—	—	1	1	1	1	2	2
1970.....	2	2	—	—	6	7	8	9
1971.....	3	5	4	4	1	2	8	11
1972.....	14	22	3	3	1	1	18	26
1973.....	22	24	3	4	1	1	26	29
1974.....	15	24	6	8	—	—	21	32
1975.....	17	20	1	1	6	7	24	28
Total	73	97	18	21	16	19	107	137

**Analysis of Cases Terminated Under the
Interception of Communications Statutes**

The statistics below exclude all nonfinal terminations such as dismissal of charges followed by the filing of a superseding indictment or information in the same case. This was done to avoid having some cases reflected in the statistics two or more times.

The statistics for fiscal year 1975 are based on data through the first nine months of the fiscal year.

		Cases Terminating in Conviction					
		Conviction After Contested Trial		Plea of Guilty or Nolo Contendere		Total	
Fiscal year	Statute	Cases	Defendants	Cases	Defendants	Cases	Defendants
1969	18 U.S.C. 2511	—	—	—	—	—	—
	18 U.S.C. 2512	—	—	1	1	1	1
	47 U)(S)(C) 605.....	—	—	—	—	—	—
	Total	—	—	1	1	1	1
1970	18 U.S.C. 2511	—	—	2	2	2	2
	18 U.S.C. 2512	—	—	—	—	—	—
	47 U.S.C. 605.....	1	1	—	—	1	1
	Total	1	1	2	2	3	3
1971	18 U.S.C. 2511	1	1	1	1	2	2
	18 U.S.C. 2512	2	2	1	1	3	3
	47 U.S.C. 605	—	—	—	—	—	—
	Total	3	3	2	2	5	5
1972	18 U.S.C. 2511	3	5	5	7	8	12
	18 U.S.C. 2512	—	—	1	1	1	1
	47 U.S.C. 605	1	1	—	—	1	1
	Total	4	6	6	8	10	14

		Cases Terminating in Conviction					
		Conviction After Contested Trial		Plea of Guilty or Nolo Contendere		Total	
Fiscal year	Statute	Cases	Defendants	Cases	Defendants	Cases	Defendants
1973	18 U.S.C. 2511	4	5	12	13	16	18
	18 U.S.C. 2512	—	—	—	—	—	—
	47 U.S.C. 605	1	1	—	—	1	1
	Total	5	6	12	13	17	19
1974	18 U.S.C. 2511	7	9	3	8	10	17
	18 U.S.C. 2512	—	—	1	1	1	1
	47 U.S.C. 605	—	—	—	—	—	—
	Total	7	9	4	9	11	18
1975	18 U.S.C. 2511	2	2	6	6	8	8
	18 U.S.C. 2512	—	—	—	—	—	—
	47 U.S.C. 605	—	—	6	7	6	7
	Total	2	2	12	13	14	15
Total Cases Terminating in Conviction		22	27	39	48	61	75

		Cases Not Terminating in Conviction							
		Dismissal by D.J.		Dismissal by Court		Acquittal		Total	
Fiscal year	Statute	Cases	Defend- ants	Cases	Defend- ants	Cases	Defend- ants	Cases	Defend- ants
1969	18 U.S.C. 2511	-	-	-	-	-	-	-	-
	18 U.S.C. 2512	-	-	-	-	-	-	-	-
	47 U.S.C. 605	-	-	1	1	-	-	1	1
	Total	-	-	1	1	-	-	1	1
1970	18 U.S.C. 2511	-	-	-	-	-	-	-	-
	18 U.S.C. 2512	-	-	-	-	-	-	-	-
	47 U.S.C. 605	1	1	4	5	-	-	5	6
	Total	1	1	4	5	-	-	5	6
1971	18 U.S.C. 2511	-	-	1	3	-	-	1	3
	18 U.S.C. 2512	1	1	-	-	-	-	1	1
	47 U.S.C. 605	-	-	1	2	-	-	1	2
	Total	1	1	2	5	-	-	3	6
1972	18 U.S.C. 2511	1	1	2	6	3	3	6	10
	18 U.S.C. 2512	-	-	1	1	1	1	2	2
	47 U.S.C. 605	-	-	-	-	-	-	-	-
	Total	1	1	3	7	4	4	8	12
1973	18 U.S.C. 2511	3	3	-	-	3	3	6	6
	18 U.S.C. 2512	1	2	2	2	-	-	3	4
	47 U.S.C. 605	-	-	-	-	-	-	-	-
	Total	4	5	2	2	3	3	9	10

		Cases Not Terminating in Conviction							
		Dismissal by D.J.		Dismissal by Court		Acquittal		Total	
Fiscal year	Statute	Cases	Defend- ants	Cases	Defend- ants	Cases	Defend- ants	Cases	Defend- ants
1974	18 U.S.C. 2511	3	4	1	1	1	2	5	7
	18 U.S.C. 2512	3	3	1	2	1	2	5	7
	47 U.S.C. 605	-	-	-	-	-	-	-	-
	Total	6	7	2	3	2	4	10	14
1975	18 U.S.C. 2511	5	6	2	2	2	4	9	12
	18 U.S.C. 2512	-	-	-	-	1	1	1	1
	47 U.S.C. 605	-	-	-	-	-	-	-	-
	Total	5	6	2	2	3	5	10	13
Total Cases Not Terminating in Conviction		18	21	16	25	12	16	46	62

**Disposition of Appeals Taken Under
The Interception of Communications Statutes**

The statistics for fiscal year 1975 are based on data through the first nine months of the fiscal year.

Fiscal year	Statute	Cases	Defendants	Disposition
1969.....		—	—	
1970.....		—	—	
1971.....	18 U.S.C. 2511	1	1	Dismissed in favor of United States
	47 U.S.C. 605	1	1	Decision in favor of United States
1972.....	18 U.S.C. 2511	1	2	Decision in favor of United States
	18 U.S.C. 2512	1	1	Decision in favor of United States
1973.....	18 U.S.C. 2511	1	1	Decision in favor of United States
	18 U.S.C. 2512	1	1	Dismissed in favor of United States
1974.....	18 U.S.C. 2511	2	2	Decision in favor of United States
	18 U.S.C. 2512	1	1	Decision in favor of United States
	47 U.S.C. 605	1	1	Decision in favor of United States
1975.....	18 U.S.C. 2511	2	3	Decision in favor of United States
	18 U.S.C. 2511	2	2	Dismissed in favor of United States

CODE OF FEDERAL REGULATIONS
Title 15 - Commerce and Foreign Trade

376.13 Communications intercepting devices

(a) Export license requirements. A validated export license is required for the export to any destination (including Canada) of any electronic, mechanical, or other device primarily useful for surreptitious interception of wire or oral communications. Any exporter who knows, or has reason to believe, that such commodities will be used for such purpose shall include that information on his application for validated export license. The application shall be on Form FC-419, Application for Export License. The words "Communications Intercepting Device" shall be entered at the top of the form immediately above the printed words "United States of America."

(b) Qualifications of exporter. Licenses to export the commodities described in paragraph (a) of this section will be issued only to:

(1) A communications common carrier or an officer, agent, or employee of, or person under contract with, a communications common carrier when engaged in the normal course of such communications common carrier's business; or

(2) Officers, agents, or employees of, or person under contract with the United States, one of the 50 States, or a political subdivision thereof, when engaged in the normal course of government activities.

(c) Examples of communications intercepting devices. An electronic, mechanical, or other device that can be used for interception of wire or oral communications is subject to the provisions of this 376.13 if its design renders it primarily useful for surreptitious listening even though it may also have innocent uses. A device is not restricted merely because it is small or may be adapted to wiretapping or eavesdropping. Some examples of devices to which these restrictions apply are: The martini olive transmitter; the infinity transmitter; the spike mike; and the disguised microphone appearing as a wristwatch, cufflink, or cigarette pack; etc. The restrictions do not apply to devices such as the parabolic microphone or other directional microphones ordinarily used by broadcasters at sports events, since these devices are not primarily useful for surreptitious listening.

(d) Effect of other provisions. (1) If, at the time of export, a validated license is also required under other provisions of the Export Administration Regulations, the application shall be submitted in accordance with this 376.13 as well as all other applicable provisions. The requirements of this 376.13 are in addition to, rather than in lieu of, other validated license requirements set forth in the Export Administration Regulations. (2) Insofar as consistent with the provisions of this 376.13, all other provisions of the Export Administration Regulations shall apply also to export license applications and export licenses for these commodities.

CHAIRMAN ERICKSON: Mr. Reynolds, we appreciate your coming. Thank you.

The meeting stands recessed until 1:30.

[Whereupon, at 12:50 p.m., a luncheon recess was taken until 1:30 p.m.]

AFTERNOON SESSION

CHAIRMAN ERICKSON: We will reconvene.

Unfortunately, some members of the Commission are going to have to leave prior to the completion of hearings this afternoon, and for that reason we will try to expedite this as much as possible.

At this time, I would like the remaining witnesses to be sworn.

Mr. Caming, I see, is at the table.

Mr. Beller, Agent Simon, and Mr. Berolzheimer.

[Whereupon, Messrs. Beller, Simon and Berolzheimer were sworn by Chairman Erickson.]

CHAIRMAN ERICKSON: The witnesses, other than Mr. Caming, may return to their seats, and we will proceed with Mr. Caming's testimony.

TESTIMONY OF H. W. WILLIAM CAMING, ATTORNEY, AMERICAN TELEPHONE & TELEGRAPH COMPANY

CHAIRMAN ERICKSON: We are fortunate at this time to have Mr. William Caming as a Commission witness. For almost ten years he has been a member of the Legal Department of the American Telephone & Telegraph Company. His responsibilities there include oversight over all legal matters pertaining to electronic surveillance, rights to privacy, and liaison with law enforcement authority.

Mr. Caming will discuss AT&T's current policies in this area and make recommendations for improvements in the law.

I understand you are going to summarize your opening statement.

MR. CAMING: Yes, Mr. Erickson.

I wish to thank the Commission for the opportunity of presenting our views, both on privacy of communication, and our various policies, practices, and experiences.

I wish at the outset to reaffirm the Bell System's long-standing commitment to privacy of communications, one which we feel very sincerely.

We have strongly opposed over the years any invasion of privacy by illegal wiretapping, and strongly endorsed legislation, both at the federal and state levels, which protected such privacy.

We believe, too, that the Federal Omnibus Crime Control Act has contributed significantly to protecting privacy by, among others, clarifying existing law and proscribing, under pain of heavy criminal

penalty, any unauthorized interception, use, or disclosure of wire communications.

Each of our Bell System companies endeavors to vigorously protect the privacy of our customers' conversations through physical protection of equipment and facilities, by advances in technology over the years, and by thorough instruction and supervision of our employees.

Any allegations of illegal activity leveled against any of our employees or any evidence thereof, whether uncovered in our day-to-day operations or brought to our attention by any outside source, is promptly and thoroughly investigated. And if the facts so warrant, prompt disciplinary and prosecutory action is taken.

Additionally, it is long-standing Bell System policy to cooperate fully with law enforcement authorities and other government agencies in their investigations of any alleged illegal activity on the part of any of our employees or others.

You have heard testimony, and I merely need to advert to the fact that yellow pages directory advertising relating to advertisements on wiretapping, eavesdropping, or debugging have long been banned for reasons set forth in my statement.

Just briefly, in the area of cooperation with law enforcement authorities, Bell System companies cooperate with duly authorized authorities by providing limited assistance as necessary to effectuate the particular wiretap order. The assistance generally takes the form of providing line access, record information such as the designation and location of the specific telephone line or lines approved for interception in the court order.

Under the federal act, in the instance of federal law enforcement authorities and in some eight states and the District of Columbia, which states have appropriate enabling laws, the court order may direct the telephone company to provide limited assistance in the form of information, facilities, and technical assistance necessary to accomplish the particular wiretap unobtrusively and with minimum disruption to service.

Our assistance generally takes the form of a private line channel from terminal to terminal, i.e., a channel from a terminal which also services the telephone line under investigation to a terminal servicing the listening post location designated by law enforcement.

We do mention our cooperation in national security matters in our statement, and I will pass on.

In cooperating with law enforcement authorities, the Bell System does provide the very minimum assistance necessary to accomplish the particular wiretap. Under no circumstances do we do the

wiretapping ourselves. That, we feel, is the exclusive province of law enforcement authorities. Nor do we furnish them with terminal equipment to be used in connection with the wiretap, such as pen registers or tape recorders, nor do we provide telephone company identification cards, uniforms, tools, or telephone company trucks.

Turning to another subject of the Commission's inquiry, disclosure of corporate toll billing record information, these are corporate records maintained by each telephone company in the ordinary and regular course of its business as necessary substantiation for charges to be billed to the customers, and required by statute. They contain no information as to the content of any telephone conversation or, with limited exception, the identity of parties to any conversation.

This information is held in strict confidence and we divulge it only under valid subpoena or administrative summons, such as that of the Internal Revenue Service.

As a matter of policy, these records are no longer disclosed pursuant to other lawful demands.

In addition, whenever such records are subpoenaed or summoned, the telephone company automatically notifies the customer within 24 hours thereafter, except when a law enforcement agency or legislative committee seeking the records specifically requests in writing that such disclosure not be made by certifying that notification could impede and obstruct its official investigation or interfere with enforcement of the criminal law.

Turning to another subject of inquiry, electronic toll fraud, in the early 1960's a most ominous threat to the telephone industry arose in the form of small electronic toll fraud devices, the so-called blue and black boxes. These devices enable the user to circumvent the telephone company's automatic billing machinery which is actuated by electrical signals, and thus the callers can place or receive free calls to or from various parts of the world.

Because these boxes are relatively and surprisingly inexpensive to make, their use has grown at an alarming rate. We estimate, for example, that blue boxes, one of which I will show you in a moment, can be produced at a cost of \$25 to \$50 per unit, and black boxes at a cost that can be as little as a dollar or so.

Our experience has also shown that these devices have a unique appeal, among others, to the criminal element, whether it be a member of organized crime or an unprincipled businessman. This is so because not only is payment of the lawful telephone charges evaded but also any record of the communication wholly concealed, permitting them to conduct their unlawful activity under a smoke screen of anonymity.

If the Commission would indulge me for a moment, I would like to just show them to you, and very swiftly go through a black box device.

The black box device is placed on the line of the telephone being called. The way it is checked—and I might say the name "black box" came about because the first one found was black as far as an outward cover—and this one, coincidentally, is marked on the back "Japan."

The wires leading from the telephone central office after they enter the home are put through here (indicating), and then brought up through here to the hand set of the telephone itself, or the receiver and transmitter.

Now, when a call normally comes in you have ringing, and you pick up the telephone, and when you do that, that off-hook condition—and the telephone line furnishes current which sends back an electrical signal to our automatic billing equipment saying, "The party has answered; the party has gone off hook, and therefore billing should commence." And it is only when that signal is received that a charge is made for the call.

The current is also indispensable in order to talk.

Now, when the call comes in through use of a black box, at the first ring the called party who controls the device will press down this button in the center. By pushing on this button he shuts off the ringing. And he then flicks the on-off switch to the "on" position, furnishing current from this device—which current is furnished by a battery contained therein—to the equipment.

So that he has done two things. He has supplied the necessary electrical current for talking circuit but also blocked the signal so that it does not go beyond this device and nothing goes back to the automatic billing machine.

So from our records standpoint, there is no record of a call having been answered.

Another interesting point: The caller, of course, is not charged for the call, since no call is completed, ostensibly.

Additionally, if he is in a coin box, which gamblers have found of great advantage, he gets his money back.

So this type of device also has appeared and we have found them in forms several inches wide, very easily concealable, very easily pocketable, and often very difficult to detect.

I will shortly just touch upon the operation of a blue box.

CHAIRMAN ERICKSON: When you do reach the blue box and compare it with the black box, would you be willing to cause a photograph to be made of the two devices of this type so it could be included in the record?

MR. CAMING: We shall be very pleased to, or if you would find it more convenient we would make the photographs and furnish them to you.

CHAIRMAN ERICKSON: We would appreciate your doing that.

MR. CAMING: And we will see that we do that next week.

MR. HODSON: Eight-by-five glossies, please.

[Laughter.]

[The material referred to follows.]

TELEPHONE COMPANY MONITORING

In addition to the types of electronic eavesdropping which the Commission has already examined, Title III contains a number of provisions which allow the monitoring of telephone conversations by persons other than law enforcement personnel. The provisions are contained in Section 2511 (2)(a)(i), which states:

"It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of any communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the carrier of such communication: Provided, that said communication common carriers shall not utilize service observing or random monitoring except for mechanical or service quality control checks."

Based on this provision, telephone company personnel may engage in the monitoring of telephone conversations. This monitoring may take one or more of the following forms:

A. Service Observing - this is the principal quality control check by which the telephone company statistically evaluates the service being provided to customers by its equipment and personnel. Incoming calls by customers to telephone business offices, repair offices, information operators and long distance operators are randomly selected, and monitoring begins, at the instant after dialing is completed but before ringing begins. The person monitoring the call is then able to determine how long it takes for the call to be answered, the quality of the connection and the nature of the service provided by the phone company representative. In addition, some customer to customer long distance and local calls are also selected for service observing, to determine the quality of service being provided by toll switching and local switching equipment. When such customer to customer calls are selected, monitoring ceases at the time that "satisfactory conversation" begins; i.e., after the salutations.

All calls monitored under the service observation program are randomly selected and the results are statistically analyzed on a continuing basis to evaluate the quality of service being provided to telephone company customers. The monitoring is conducted from secure locations by experienced telephone company personnel.

B. Supervisory Monitoring - this practice is engaged in by the telephone company, governmental agencies and private concerns.

The purpose of supervisory monitoring is to evaluate the quality of service being provided by persons handling incoming telephone calls from the public.

Supervisory monitoring differs from service observing in several important respects. While service observation is designed to provide a statistical analysis, supervisory monitoring is designed to actually evaluate the performance of specific individuals. Furthermore, supervisory monitoring is not limited to the phone company; under a theory of implied consent, governmental agencies (such as IRS Tax Information Centers) and private concerns (such as airline reservation offices) also engage in such monitoring, using equipment provided under tariff from the telephone company.

Only incoming business calls are subject to supervisory monitoring and while the employees are aware that their telephone performance may be monitored, the calling party is generally not aware that his conversation may be overheard by supervisory personnel. Because of this, the regulatory bodies in at least two states have prohibited supervisory monitoring unless the calling party is given advance notice that his call is subject to monitoring.

C. Electronic Toll Fraud Investigations - Since the early 1960's, small electronic devices have been manufactured and distributed through black market channels which are capable of electronically overriding the telephone company's automatic billing equipment, enabling the user to make long distance telephone calls at no cost. A "blue box" is used by the calling party; a "black box" by the called party, but in both cases the telephone company is defrauded out of long distance revenues.

The detection of blue and black box usage by telephone company security departments is difficult, but not impossible. Blue box users, in order to gain access to a long distance line, must begin by dialing a toll-free (800) number. Before the called number actually rings, the user presses a button on his device which produces a specific multi-frequency electronic tone. This tone not only switches the call from the originally dialed number onto an open long-distance trunk, but also overrides the company's automatic billing equipment. The user is then able to dial any area code and number, stay on the line for as long as desired and not be billed for the call. The telephone company's only record of this usage is that it will show up as a call to the originally dialed toll-free number and will show how long the call lasted.

Telephone company security departments look for patterns of frequent, lengthy calls to toll-free numbers as preliminary evidence of electronic toll fraud. Once such evidence is obtained, an electronic device can be attached to the suspected line which, by analyzing the electronic tones and signals on the line, can determine with a high degree of reliability, whether electronic toll fraud is being committed.

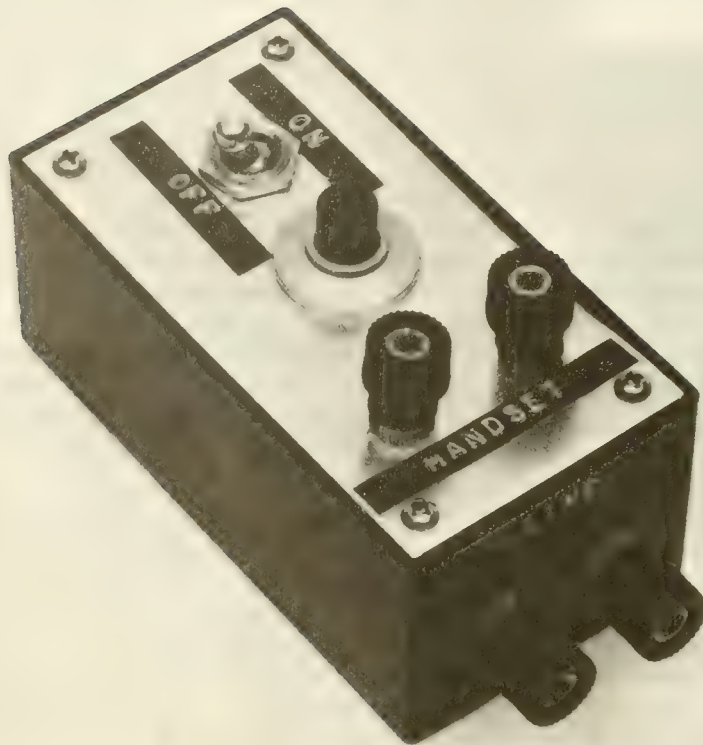
Under the exception provided in Section 2511 (2)(a)(i) for "any activity which is a necessary incident...to the protection of the... property of the carrier of the communication," many telephone companies have engaged in the monitoring and recording of customer to customer conversations over lines where electronic toll fraud is suspected. The statutory exception is broad and absolute; no court order is necessary and no law-enforcement participation is required, even though the intent of the monitoring and recording by phone company personnel is to secure evidence of criminal activity.

Perhaps the broadest interpretation of this provision was given by AT&T who used it to justify the continuation of a program, begun in 1964, whereby as many as 40 million customer to customer calls were electronically "scanned," and up to 2 million recorded and analyzed, in an attempt to determine the statistical frequency of electronic toll fraud. This particular program was ended in mid-1970. (See attached newspaper account, the details of which were confirmed to the Commission staff by an AT&T representative.)

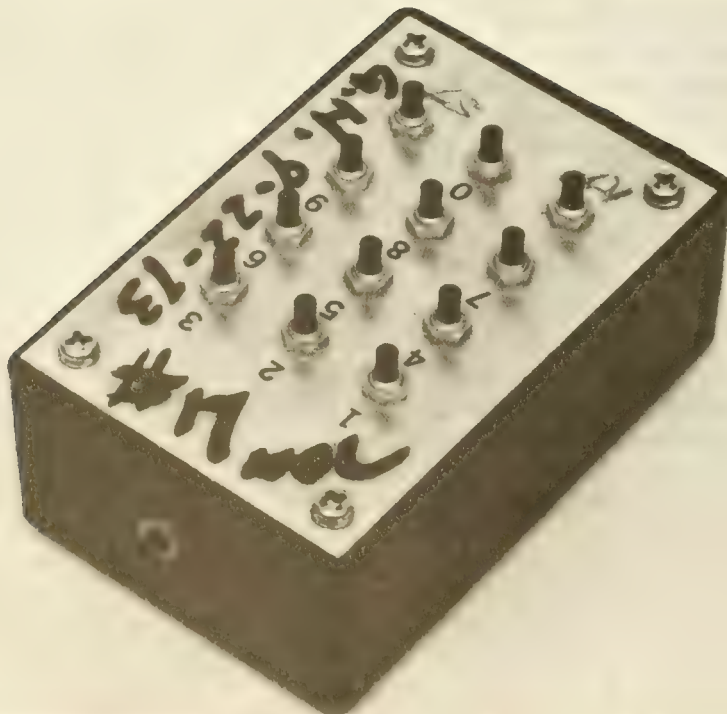
There is currently a proposed amendment before Congress which would prohibit the telephone company from monitoring conversations in electronic toll fraud investigations. The effect of this amendment would be to require the company to bring law enforcement personnel into the investigation and have them secure a court order, under Title III, before any voice monitoring could take place, or else to conduct their investigations without monitoring.

In order to fully explore both sides of this question, the Commission will hear from a representative of AT&T, Mr. H.W. William Caming, who will defend the practice of telephone company monitoring without a court order, and from a representative of The Central Telephone Company, Mr. Neil Beller, and an FBI agent, Michael Simon, who successfully investigated and prosecuted several blue box cases in late 1973, in Las Vegas, Nevada, without monitoring customer conversations.

BLACK BOX



BLUE BOX



Bell Secretly Monitored Millions Of Toll Calls

By LOUIS J. ROSE
Of the Post-Dispatch Staff
1975, St. Louis Post-Dispatch

The Bell Telephone System monitored in random fashion millions of long-distance calls originating in six cities, including St. Louis, and secretly tape-recorded parts of at least 1,500,000 calls for analysis in New York.

The Post-Dispatch has learned that the highly secretive program was designed to help combat electronic toll call frauds, but only a tiny fraction of the calls listened to and recorded were ever confirmed by the company as being fraudulent.

Other cities besides St. Louis where calls were monitored were New York, Detroit, Miami, Los Angeles and Newark, N. J.

The monitoring program covered a six-year period and ended in the spring of 1970, when those Bell executives involved were warned to purge their files of any reference to the program and to destroy any materials relating to it.

A source with knowledge of the internal operations of the Bell system said that Bell executives who ran the monitoring program believed the company was within its legal rights, but were afraid Bell's image might be damaged if word leaked to the public.

"From the beginning they analyzed this very carefully," the source told the Post-Dispatch, "and decided that if it ever were necessary to reveal the existence of this equipment in order to prosecute a toll fraud case, they would simply decline to prosecute."

A good percentage of the tape recordings involved segments of from 30 seconds to 90 seconds from the time a call was first dialed, but in several hundred thousand instances entire conversations were recorded.

The monitoring equipment frequently misread calls as having indications of electronic toll fraud. Certain frequency components in human speech, for example, could have caused the equipment to be activated as if fraud were involved, with the result that the entire conversation might be taped, it was said.

The program was unknown to many

high-ranking Bell executives even in areas where it was in effect.

More than 30,000,000 long-distance calls were monitored during the first four years of the program by sophisticated equipment that scanned trunk-line calls. The equipment looked for electronic indications that an attempt was being made to bypass the system's toll charge mechanism.

Of the more than 1,500,000 long-distance calls that were at least partly recorded during the first four years of the program, with the tapes being sent to New York for analysis, fewer than 25,000 were considered by those doing the analysis to be indicative of fraud.

Fewer than 500 of the calls in this category during the first four years were confirmed as fraudulent.

Initially, the program went into effect in late 1964 with six units, each capable of monitoring 100 trunk lines. Each unit could handle about five calls at any given moment. The program began with two units each in New York and Los Angeles and single units in Miami and Detroit.

Early in 1967, the Detroit unit was transferred to St. Louis. It was installed here at the Southwestern Bell facility at 2651 Olive Street, remaining there until the spring of 1970. It was about then that the entire program was ended.

Several factors, including fear of public exposure, figures in the decision to end the program. Other factors, included concern over the condition of the monitoring units and whether the whole approach was efficient and comprehensive enough.

Joseph F. Doherty, who is now director of corporate security at the New York headquarters of American Telephone & Telegraph Co., played an important role in the program and was among those involved in the orders that files relating to it should be purged and destroyed.

Doherty, when asked for comment, suggested that a reporter channel his questions through public relations personnel at Southwestern Bell Telephone Co. here, one of 22 AT&T companies

Later Friday, William Mullane, press relations director for AT&T confirmed most of the details known to the Post-Dispatch. Mullane said the program largely was an experimental or trial project and was ended May 1, 1970.

He said he did not know how many calls had been tape-recorded, but said he believed the recordings ran between 60 and 90 seconds. The Bell system continues to crack down on electronic toll fraud, but its present approach does not involve voice recordings, he said.

The monitoring units used during the old program were designed by Bell Laboratories to detect electronic toll cheaters, particularly those persons who utilized "blue box" and "black box" equipment.

(A blue box is a device intended to allow the user to place long-distance calls that dodge the Bell system's billing equipment. A black box is a device that enables persons to call the box's owner long distance without paying for the call.)

The monitoring units worked this way:

Once the unit locked onto a call, it would record on a temporary recorder the initial phase of each call. If it found nothing indicating electronic fraud, the temporary recording was erased and the equipment prepared to handle a new call.

But if the initial phase appeared to indicate, for example, that a blue box was being used, the equipment activated a master tape recorder that would record a segment or the entire content of the call. The master tape subsequently was sent to New York for analysis.

Mullane said that elaborate precautions were taken to assure that the tapes were studied only by a small group of trained security personnel in New York. "They could not be listened to locally," he said.

He conceded the program had been kept highly secretive.

"The fewer people that know anything you are doing to detect fraud, the better off you are," he commented.

MR. CAMING: When we were faced with this problem the first time, we were faced with the fact that if fraud could be committed with impunity by the caller and called party, and a large number of these inexpensive devices could flood the market, staggering financial losses would naturally ensue.

Faced with this threat, the Bell System took immediate steps in the early '60's to determine whether it would be necessary to undertake what was a monumental task of redesigning and restructuring the signalling functions of the nationwide telecommunications network, at an estimated cost to our customers which would range upwards from a half-billion to a billion dollars, as well as taking several years to accomplish.

We, therefore, took steps to determine the magnitude of the fraud through instituting a very limited action strictly controlled and rigidly guarded experimental program of scanning and testing the network at only several key representative cities—no more than five at one time—between late 1964 and early 1970, to which reference has been previously made.

Now, we did examine in this area a limited number of trunks, by having the telephone equipment fastened to 100 trunks at each of these five representative locations. In one or two places they were moved to more representative positions. And we could only sample—and it was random sampling—five calls at any one time.

These calls would be mechanically scanned, tested, and looked at by the equipment—there was no human ear involved—and determined whether they were legitimate. It was like putting your hand into a stream, picking out a fish, examining it, and then dropping it back into the stream.

The scanning, testing, and recording were done by mechanical means. If the call appeared legitimate, that is, if the proper supervisory signals were present, then the call would be immediately thrust back.

However, if the call showed preliminary indications of illegality, that is, it looked to the equipment to be an illegal call—that is, one basically of two types: if you could hear voices but there was no current seemingly going to the call and therefore no billing, that was an indication of a black box call. Or if there was a telltale blue box tone, which would be used to seize the network by the caller, that, too, appeared to be an illegal call.

In such cases, and only in those cases, were the calls recorded by equipment associated with this scanning equipment.

The recordings were for limited periods, and this, too, was done by mechanical means.

The equipment that did result in the recording was under very secure conditions, and the recordings were sent for analysis to the Analysis Bureau in New York to insure that there was very limited scrutiny, and particularly examined, for two purposes: One, the attempt to determine the statistical magnitude of the fraud, as I mentioned earlier, and secondly, in some cases to determine whether there were any leads as to who the caller or called party might be.

Now, this was first-generation type of equipment which we recognized and was done for the purpose basically of determining the magnitude of the problem.

We were simultaneously working on second-generation equipment, and also working on other methods of detection. And by early 1970 we had reached a stage where we would discontinue the very limited voice recording that went on. As a result, all recording was terminated in this preliminary indication, scanning-of-the-network stage, in May of 1970.

Since then, we have been using effective scanning and testing procedures which have eliminated the necessity of any voice recording during the pre-investigative, as I characterize it, preliminary detection stage of examining the network. These have included extensive use of computers, plant-testing equipment and procedures, and statistical analysis of traffic patterns, and development of more sophisticated network scanning equipment which does not require any voice recording capability.

Just for a moment, the Communications Act imposes on all telephone companies the obligation by statute to prevent such thefts of service. Prosecution has been and continues to be, in our opinion, the only effective deterrent. A minimum amount of recording of a very limited number of illegal calls is still indispensable in a substantial number of cases during the last evidence-gathering investigative stage.

But we are most concerned and have full recognition of the public concern in this area. So to assure to the maximum possible degree the privacy of communication, we employ a series of investigative measures other than voice recording, such as, for example, after getting preliminary indication of illegality, we will use a measuring device, such as a peg count register or its equivalent, which will indicate the telltale tones by recording them on paper tape or a counting mechanism so we can carefully further evaluate the accuracy of any preliminary indications of electronic toll fraud.

Only when a reasonably strong suspicion of such fraud has been firmly and unequivocally

established, the possibility of any plant trouble ruled out by proper testing, and all other investigative measures exhausted, do we engage in limited recording.

And now we come to the blue box, if I may.

The blue box is the more commonly known box, and its function permits greater flexibility as far as accomplishing theft. As you can see, it is very small. It is portable. You can literally put it in your shirt pocket and be undetected. And this one, too, coincidentally, bears on the back of the case, "Japan."

Normally when you place a call to any of a series of numbers—for example, if you call in a distant city information, which would be in Washington 212 and the traditional 555-1212, you would be making what would be called a noncharge call. This means that when you make the call the equipment will record the call but will not bill it to the customer on the automatic billing equipment.

Just to give you a very simple explanation of how our billing equipment works: When you pick up your own telephone as the caller, an off-hook condition is noted in our automatic billing equipment. Then, after you dial the number and all, and the called party answers, a second entry is made in the equipment. And this might be 200 entries later in a busy metropolitan area, because whatever entry is made with different phones going off the hook are recorded in this continuous process and later the computer coordinates the information for each call.

Then, at the completion of the call, when the called party hangs up, there is a third entry. You have time and distance which are the two factors, and then statutorily required billing charges.

When you make a free call, there are the same entries but there is a no-charge condition.

What happens is you may make a call to information or an 800 number, which is a no-charge number, such as calling Hertz or Sears-Roebuck in a distant city, or you may call the business office of the telephone company.

Now, here is how this box would work—and it is quite simple. The party first dials, say, Chicago, which is 312-555-1212. They dial that on their regular telephone and it goes through the network and you can sort of hear it progressing from your listening. And then you hear the ringing cycle, meaning it is in Chicago at the switching center.

But before the party answers, you then emit the telltale tone (indicating) that is a signal to the equipment that dislodges the call and literally seizes the circuit. It is an internal signal that we use to indicate the circuit is free.

As soon as that is done—and you are now in the toll network, not in the portion going from the local

telephone to the local central office, but the actual intercity or more than one central office toll network. There is no reason to have this telltale tone present unless it just happens to be accidentally present during a conversation when that frequency is emitted by some sound in the background.

So after you seize it at Chicago you press the KP, which is the key pulsing button that only a toll operator has.

Then you dial, in Sydney, Australia, say, whatever number you want to, using the code—in the United States or in Sydney or in London. And when you have dialed all that, then you press another button which only the operator has, the start button, and it appears to the equipment that another long-distance call is coming through, so you at Chicago, having seized the circuit, send the call on to its destination.

Now, when the call is completed and your party in Sydney picks up the line, the equipment, not having recognized that an alien body has seized it from distant planets, thinks that you have completed your call to information in Chicago. So all you have at that point is an entry that you reached the information operator—a no-charge condition. Then when your party in Sydney, Australia, hangs up, the equipment thinks that the information operator, directory assistance operator in Chicago, has hung up. And that is all that shows.

Meanwhile, if you have any facility with this—and as you see, it is acoustically coupled so you don't have to connect it in any way with wires or hard wire—you can then do this (indicating) and start your next call.

So you don't even have to redial Chicago. You can stay on this, controlling the Chicago line that you have seized, and make a series of five or ten calls to all parts of the world. And if you make your next call within a period of seconds after the first call, you are off again. The equipment still thinks, "This fellow is talking a heck of a long time to that directory assistance operator in Chicago."

CHAIRMAN ERICKSON: That blue box, as you denominate it, has a sticker on it. Was this an exhibit in some case?

MR. CAMING: Yes. This was a grand jury exhibit in a particular case on October 24, 1973, and at the conclusion it was provided by the court to us.

CHAIRMAN ERICKSON: Was a conviction obtained?

MR. CAMING: I believe it was. I am not sure with certitude in this particular case, but our batting average has been rather good because we are rather careful before we bring anything to prosecution.

Now, what do we record? Remember, we don't do any recording at all until every other investigative method has been carefully explored, and until we have established by other equipment that this is definitely an illegal call. In other words, we would keep a count, for a day or so, by a counting mechanism of one type or another of the number of times, plus perhaps the various tones dialed, indicating that there was undoubtedly a blue box being used.

Once we have established this and are in our final evidence-gathering stage, the recording is very brief and usually includes three facets: The dialing of the multi-frequency tones of the blue box after the tell-tale tone of the blue box is emitted. That actuates the equipment. It does not start until then.

And we would record the dialing tones and then the ringing cycle of the fraudulent call and the opening salutation when the party answers. Generally this entire process is 60 seconds or less of voice conversation, and very often it is only 60 seconds for the entire recording, including the ringing and dialing facets.

Now, as part of our continuing concern and review of our operating policy relating to privacy of our communications, we recently have further refined our procedures to require that no such limited recording may take place unless the prior express approval is obtained of the company's Security Manager and the concurrence of the Vice-President, Operations, and the Vice-President and General Counsel of a particular company, or their designee. In this respect, too, as in many others, our systemwide procedures, as in toll billing records and in most of our procedures, are more restrictive than the requirements of the law but reflective of our concern.

Now, I might just say in passing that these crimes have never enjoyed the protection of the law, neither before nor after the passage of Title III. It is of particular interest, though, that almost all these cases go to prosecution, and in these cases our entire process of evidence-gathering has been subjected to close and thorough judicial scrutiny and, of course, a confrontation by the defendant.

This judicial oversight has continued to date with some 325 convictions and a number of pending cases, which indicate not just the number of convictions but the extent to which courts at state and federal level have repeatedly reviewed our procedures for gathering evidence.

With virtual unanimity, the courts have held the methods have been lawful, have been effected independently of cooperation with law enforcement authorities, and are in the public interest.

Now, we have introduced a federal statute proscribing the manufacture, possession, importation, distribution, or advertising of these devices, and the publication of plans, specifications, and instructions for making or assembling or using them. And we have submitted that to the commission for its consideration.

We feel it would substantially contribute to the containment of this type of fraud. Prosecution for illegal use under a statute such as the fraud-by-wire statute will, of course, continue to be our first line of defense. But a statute of this character would do a great deal to assist.

Now, as in many criminal areas, detection here is very difficult. And the instances of electronic toll fraud that we know about, I think I can frankly say, represent the portion of the iceberg that meets the eye.

We believe that the actual losses currently being sustained by us may be ten or twenty times as great as the profitable losses which we calculate to be on the order of a million dollars or more a year.

Now, we feel, in concluding, that the virtually unchecked use of electronic toll fraud devices which would result if the threat of effective detection and prosecution is removed would impose an overwhelming financial burden on the telephone industry.

You can visualize what would occur if every household had a blue box and a black box. It would require the telephone industry and its honest customers to underwrite the entire cost of these depredations, not only the loss of revenue but the substantial expense of the circuits, facilities, and equipment which are tied up by such illegal use. And these losses would rapidly reach staggering proportions, soaring into the tens and hundreds of millions of dollars, and I think it's fair to say jeopardize our very ability to provide telephone service to this nation.

I would be very pleased to answer any questions that the Commission may have.

CHAIRMAN ERICKSON: We appreciate that very much, Mr. Caming.

Mr. Feldman will proceed with the questioning.

MR. HERSHMAN: If you don't mind, I have just a few questions I would like to ask before Mr. Feldman begins.

At the request of the Commission you supplied us with figures indicating that between January 1, 1967, and June 30, 1974, approximately 1,457 devices were found on the facilities of AT&T and its subsidiaries. Could you tell us, Mr. Caming, how these devices were found?

MR. CAMING: I take it by that you mean who found them?

MR. HERSHMAN: Who found them and in what course of business?

MR. CAMING: Well, as you might well anticipate, Mr. Hershman, they were found in a variety of ways. A great many of them were found by our own telephone people routinely in the course of their day-by-day duties.

We have, for example, some 90,000 Bell System outside-plant personnel who are continuously in contact with the plant, both the outside facilities and in offices and homes. And, of course, there they have on a large number of occasions found these devices.

In addition, whenever a customer requests a plant check for a possible wiretap, we make as exhaustive a search as we possibly can.

Now, admittedly many of these supposed wiretap complaints we can establish are plant troubles, such as static, as I mentioned in my statement, or crackling noises or voices on the line. But if we cannot, we then make a very thorough physical inspection, and frequently the devices have been found as a result of a customer check.

MR. HERSHMAN: How frequently would you say, Mr. Caming?

MR. CAMING: I would not offhand know, but I would say that both methods are contributive to the totals that were achieved. I have no idea of the breakdown, and I don't think it would necessarily control. In both cases the telephone company has found it and our people are very alert to any irregularity or foreign device and are instructed to report immediately.

Now, many times we ourselves determine that it is not what it appears to be. For example, you may find a loose wire and it turns out that it was just left there by a previous installation being closed off.

But we are continually refining our methods. We make a very exhaustive investigation of every complaint. We do not take any of these lightly. We very carefully explore them.

MR. HERSHMAN: Mr. Caming, how many examinations of this nature do you make a year?

MR. CAMING: I beg your pardon?

MR. HERSHMAN: How many searches of this nature do you conduct each year?

MR. CAMING: I would say that we receive in the order of 10,000 complaints, as an average, in the Bell System over a year. And in addition to that, there are, of course, the 90,000 craftsmen that are out every day. And they themselves just regularly keep their eyes open.

MR. HERSHMAN: Mr. Caming, do you have a breakdown of the number of devices found after the initial call from a customer to have his wires checked?

MR. CAMING: I do not know offhand. We could check that out. I do not know whether we do maintain records of that character. The reason I say that is that when we get a request for a check, a wiretap check, in the very, very large proportion of the cases, well over 90 per cent, we can establish through central office testing that these are nothing more than plant difficulties so there would be no reason to keep any check of it. We just advise the customer that we have corrected the condition and found what it was.

So it is only a small percentage that really turn out to require further investigation than the central office electronic testing.

MR. BLAKEY: Mr. Caming, the reason these questions are being asked is there is testimony in our record from private detectives that they found a certain number of devices out of a certain number of checks. Some have indicated as high as one in five.

And, frankly, your experience is something against which we can examine the private detectives' experience. If you have records that would indicate how many times you find devices out of how many times you go out to the house and the phone to look, then we have some objective test as against the private detective statements. And if the material is relatively easily retrievable, it would be of assistance to the Commission.

MR. CAMING: We will certainly check that, Professor Blakey, and if we do keep such records we will, of course, be very pleased to present them to the Commission.

I would say offhand, just based on my own experience, that the figures sound rather on the high side.

MR. BLAKEY: If you don't have the figures exactly, could you—

MR. CAMING: Estimate?

MR. BLAKEY: —cause a reasonable survey to be made of your knowledgeable people and give us the benefit of your best estimate?

MR. CAMING: We will check all of our companies' security departments and plant departments to insure we will either give you the accurate figures or a very close reflection based on our experience.

MR. HERSHMAN: That would be most helpful, Mr. Caming.

The figures that you supplied to the Commission gave specifics on approximately 1,009 devices found since January 1967. Of these devices found, a great majority were reported to law enforcement. However, there still remains a somewhat substantial number that weren't reported to law enforcement, and I would like to know what your policy is and why it was not reported to law enforcement.

MR. CAMING: If I remember the figures off the top of my head, I think 88 per cent or 87.9 per cent of the figures we gave you were reported to law enforcement authorities either at the federal or state level.

And I might, by way of just commentary, say I noticed a newspaper article that commented that only 661 were reported to the Federal Bureau in our figures to you.

MR. HERSHMAN: I believe that was 610.

MR. CAMING: You have the advantage.

MR. HERSHMAN: For the record.

MR. CAMING: But roughly that number. One of the reasons for that is that in many areas—it may not well be appreciated—we react to the requests of local law enforcement whom to report them to.

For example, in New York City in the Queens area, we have been asked by the Bureau to report them to the local district attorney who then filters them, and only those that appear to be of federal interest are reported to the federal authorities.

This accounts for the fact that our total figure is higher than our figures to the Bureau.

We usually report them to whichever agency it is the desire mutually of the appropriate federal, state, and local authorities that we do report it to.

Secondly, of the 12 per cent, it must be appreciated that about 8 per cent of those reflect earlier cases, many of which were situations where the devices were found in remote areas or in satellite—well, in some cases they were found in domestic cases, marital cases, and with the express wish of the parties involved that they not be reported.

I think that accounts for all but about 4 per cent.

Now, our policy itself is to report every case to law enforcement authorities. We do that now generally in all companies with one exception, where they do not report it except with a prior authorization of the customer. And this has been based upon long-standing concern for the fact that the customer may in many instances, because of domestic situations, not desire it. We have urged that company to reconsider its position.

MR. HERSHMAN: Which company is that?

MR. CAMING: It is Illinois Bell Telephone Company. And I think that accounts for 4 of the 12 per cent we are talking about.

But it is Bell System policy that it be reported, and generally it is reported in all cases, both to the customer and to law enforcement.

MR. HERSHMAN: Nonetheless, if the customer requests that it not be reported, then—

MR. CAMING: In the case of Illinois Bell, they report it only if the customer requests it or they tell the customer that they will be very pleased to

cooperate fully with law enforcement if the customer wishes them to go forward with it.

MR. HERSHMAN: If Congress took steps to mandate the reporting of all illegal devices to law enforcement authorities, would that bother you greatly?

MR. CAMING: Would that bother us greatly?

MR. HERSHMAN: Yes.

MR. CAMING: Not at all. It is the Bell System policy.

MR. HERSHMAN: Except in Illinois.

MR. CAMING: Except in Illinois, and I think I can say that if the Commission expresses grave concern on that—

MR. HERSHMAN: Oh, I think the Commission does.

MR. CAMING: —we in talking to our confreres in Illinois Bell will bring that to their careful attention.

MR. HERSHMAN: My personal opinion is that it is the responsibility of the telephone company when a device is found to report it to law enforcement.

MR. CAMING: It certainly is a policy that we subscribe to and one which we have very carefully followed, with the exception of Illinois Bell which requires the prior authorization of customers at this time.

MR. HERSHMAN: Mr. Caming, we had testimony yesterday from a private investigator in the Los Angeles area who was quite disturbed that he was not allowed to advertise his debugging services in the yellow pages. He expressed his belief that one of the motivations the telephone company has in not allowing debugging services to advertise was because they were afraid debuggers would eventually find illegal wiretapping conducted by the telephone company.

For the purpose of these hearings and our record, I would like you to explain exactly why it is you do not allow debuggers to advertise.

MR. CAMING: I'd be very pleased to.

It was in the early '40's or so when wiretapping was declared illegal that we banned all advertising relating to wiretapping from the yellow pages as publishers of the directories.

In the mid-'60's, during the consideration of the Omnibus Crime Control Bill, and after the Long committee hearings of the Subcommittee on Administrative Practices and Procedures had been initiated, we decided as part of our continuing review that we would ban all eavesdropping advertising, too, although up to that date it was not a federal offense. I think the FCC had then recently declared it, from the regulatory standpoint, proscribed in radio communications, but it was not a federal offense, and many states did not so consider eavesdropping.

But we felt it a matter of responsibility, as responsible publishers, and also because of our concern and the public's concern for privacy of communications, we banned eavesdropping and also felt it was appropriate to ban debugging, because those who have a capability, as I mentioned in my statement, to debug, also have the potential to become wiretappers and eavesdroppers.

And it was our experience reflected in our yellow pages, too, over the prior years, that a number of private investigators, for example, advertised that they would both wiretap and debug.

We were fearful, therefore, that by eliminating wiretapping and eavesdropping advertising, the name "debugging" would become a synonym for what we had eliminated, and reflect to those who were looking for someone who was wiretapping an indication that this person had the capability.

MR. HERSHMAN: Has this been challenged in the courts, Mr. Caming?

MR. CAMING: It has. We had a very extensive case in the St. Louis area before the Missouri Public Service Commission, and I believe also it may have gone into court, in which our policies were challenged and expressly upheld by the Missouri Public Service Commission as being in the public interest, and also within our province as publishers.

MR. HERSHMAN: Mr. Caming, would you kindly supply the Commission with a letter concerning the details of that case?

MR. CAMING: I can do better than that. I will send you a copy of the decision.

MR. HERSHMAN: I would appreciate that.
[The material referred to follows.]



American Telephone and
Telegraph Company
195 Broadway
New York, N. Y. 10007
Phone (212) 393-9800

March 18, 1975

Mr. Kenneth J. Hodson
Executive Director
National Commission for the
Review of Federal and State
Laws Relating to Wiretapping
and Electronic Surveillance
1875 Connecticut Avenue, N.W.
Washington, D.C. 20009

Dear Mr. Hodson:

As promised at our meeting of March 5, 1975, enclosed for your information and that of your Staff is a list of citations of representative judicial decisions upholding the lawfulness of the methods employed by Bell System Companies (including limited recording) in gathering evidence, for billing and prosecutory purposes, of the commission of electronic toll fraud, accomplished through the use of devices such as the so-called black and blue boxes. These cases span a period from the mid-Sixties to the present. They uniformly hold that the illegal "placing" of calls through the use of these devices was not protected, either under § 605 of the Communications Act of 1934 or under the Federal Omnibus Crime Control and Safe Streets Act of June 1968.

The Courts have stated that the Communications Act imposes upon common carriers the statutory obligation to prevent such thefts of service. In essence, all users of telephone service must be required to pay the lawful, tariff-prescribed charges. No carrier may discriminate between its customers by granting preferential treatment to any. Knowingly to allow those committing electronic toll fraud to receive "free service" would constitute such discrimination and be violative of the carrier's statutory duties. [See §§ 202, 203(c) of 47 U.S.C.] Further, each telephone company is enjoined, under pain of criminal penalty, from neglecting or failing to maintain correct and complete records and accounts of the movements of all traffic over its facilities. [§ 228 of 47 U.S.C.]

These cases are illustrative of the judicial holdings at federal and state level to the effect that such

crimes have never enjoyed the protection of the law, neither before nor after the passage of Title III of the Federal Omnibus Crime Control Act. A substantial number of distinguished courts, including several United States Circuit Courts of Appeals, have uniformly held that persons stealing telephone service by trespassing upon the telephone network place themselves outside the protection of § 605 of the Communications Act and of Title III.

In these criminal cases, the telephone companies' methods of gathering evidence has been subjected to close and thorough judicial scrutiny and oversight. With virtually unanimity, the courts have held that the methods used have been lawful, independent of cooperation with law enforcement authorities in the evidence-gathering stage, and wholly in the public interest. Further, such evidence gathering was not violative of the Fourth Amendment or other constitutional strictures.

These cases are to be associated with and are supportive of the Statement that I presented in behalf of the Bell System to the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the House of Representatives Committee on the Judiciary on February 18, 1975.

* * * * *

Also enclosed is the requested annual tabulation for the period 1961 through October 1974 of the persons arrested at federal, state and local levels for and those convicted of the commission of electronic toll fraud through the use of devices such as the so-called blue box and black box. In the aggregate, there were some 468 arrests and 267 convictions. It is my understanding, however, that there were virtually no acquittals. Apart from those convicted, most of the others arrested had their cases disposed of, at the discretion of the particular prosecutor, without indictment, information or trial. With respect to those not prosecuted, restitution was often made, cooperation often obtained in the form of information as to the source of the device, and recovery of the device itself frequently effected.

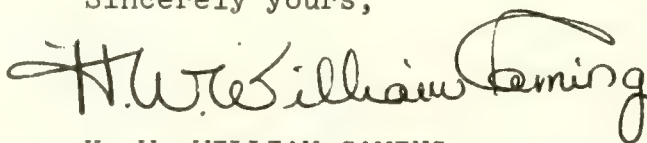
The arrest and conviction figures may be somewhat understated, since centralized statistics were not fully maintained prior to 1971. Furthermore, in these early years, it was Bell System policy not to seek prosecution except in a few major cases. Instead, deterrent interviews were conducted by the telephone companies without recourse to law enforcement authorities.

Mr. Kenneth J. Hodson

Also included is a breakdown of the 1036 blue and black boxes recovered during the foregoing period, 606 of which were blue boxes and 430 of which were black boxes. Again, these figures are not all inclusive. Additionally, other types of electronic devices, such as the cheese box and red box, have also been recovered.

Should you have any questions with respect to any of the foregoing, I shall be pleased to discuss them with you.

Sincerely yours,

A handwritten signature in dark ink, appearing to read "H. W. William Caming". The signature is fluid and cursive, with a large, looping initial "H" and a long, sweeping tail on the "g".

H. W. WILLIAM CAMING
Attorney

Enclosures

CITATIONS OF REPRESENTATIVE JUDICIAL DECISIONS
UPHOLDING THE LEGALITY OF THE METHODS EMPLOYED BY
ASSOCIATED OPERATING COMPANIES OF THE BELL SYSTEM
TO GATHER EVIDENCE (INCLUDING LIMITED RECORDING),
FOR PROSECUTORY AND BILLING PURPOSES, OF THE
COMMISSION OF ELECTRONIC TOLL FRAUD THROUGH THE
USE OF SO-CALLED BLUE AND BLACK BOXES OR
OTHER ELECTRONIC DEVICES

United States v. Sugden, 226 F.2d 281 (9th Cir. 1955), aff'd per curiam, 351 U.S. 916 (1956)

United States v. Beckley, 259 F. Supp. 567 (N.D. Ga. 1965)

United States v. Hanna, 260 F. Supp. 430 (S.D. Fla. 1966), aff'd upon reh., 404 F.2d 405 (5th Cir. 1968), cert. denied 394 U.S. 1015 (1969)

Brandon v. United States, 382 F.2d 607 (10th Cir. 1967)

United States v. Kane, 450 F.2d 77 (5th Cir. 1971), cert. denied, 405 U.S. 934 (1972)

Nolan v. United States, 423 F.2d 1031 (10th Cir. 1970), cert. denied, 400 U.S. 848 (1970)

Bubis v. United States, 384 F.2d 643 (9th Cir. 1967)

United States v. McDaniel, unreported Memorandum Decision (9th Cir. 1974), copy of which is attached, distinguishing Bubis supra.

United States v. Baxter, 492 F.2d 150, 166-67 (9th Cir. 1973)

Katz v. United States, 389 U.S. 347, 352 (1967)

Burdeau v. McDowell, 256 U.S. 465 (1921)

United States v. Shah, 371 F. Supp. 1170 (W.D. Pa. 1974)

United States v. Freeman, 373 F. Supp. 50 (S.D. Ind. 1974)

United States v. DeLeeuw, 368 F. Supp. 426 (E.D. Wisc. 1974)

United States v. Jaworski, 343 F. Supp. 406 (D. Minn. 1972)

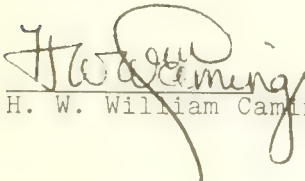
People v. Garber, 275 Cal. App. 2d 119, 80 Cal. Rptr. 214 (Ct. App. 1st Dist. 1969), cert. denied, 402 U.S. 981 (1971)


H. W. WILLIAM CAMING
Attorney

March 18, 1975

STATISTICS ON ARRESTS AND CONVICTIONS OF
PERSONS COMMITTING ELECTRONIC TOLL FRAUD AGAINST
ASSOCIATED OPERATING COMPANIES OF THE BELL SYSTEM,
INCLUDING A TABULATION OF CERTAIN ELECTRONIC TOLL FRAUD
DEVICES RECOVERED

<u>YEAR</u>	<u>PERSONS ARRESTED</u>	<u>PERSONS CONVICTED</u>	<u>RECOVERY OF "BLUE BOX"</u>	<u>"BLACK BOX"</u>
1961	39	39	4	279
1962	1	1	2	2
1963	7	7	16	2
1964	29	28	42	5
1965	11	13	20	12
1966	14	8	19	14
1967	13	2	28	4
1968	11	1	9	7
1969	3	3	5	8
1970	6	4	16	13
1971	43	35	27	32
1972	57	26	59	8
1973	119	66	217	29
1974 through October 31	<u>115</u>	<u>34</u>	<u>142</u>	<u>15</u>
TOTAL	468	267	606	430


H. W. William Caming

MR. CAMING: Yes.

And it has been our general experience that anyone that wants a reliable debugging concern—and it is no reflection upon those in many reputable concerns—can readily obtain it from other sources, such as the local police department or the local Federal Bureau of Investigation, or perhaps the chamber of commerce, who can establish the soundness of the reputations of the firms.

Does that answer your question?

MR. HERSHMAN: Yes, it does.

MR. WESTIN: Mr. Hershman, I'd like to ask a question about that, please.

Just so I understand the framework in which your answer was made, is it your position that you do not accept for advertising in the yellow pages any advertisement which is against public policy, though it is not expressly illegal? For example, would an abortion ad, prior to legalization in the state, have been refused by you and now would it be accepted by you?—so I get some perspective on it.

MR. CAMING: No, Professor Westin. I was addressing myself not to public policy but to the fact that it is our belief that in the very delicate area of privacy of communications, where we, long before it was illegal, banned eavesdropping advertising—you see, it was in December of '66. The Crime Control Act was passed in June of '68. We, on our own, did this and, to insure there was no loophole in the ban against wiretapping and eavesdropping, simultaneously refused to any longer take debugging ads.

MR. WESTIN: My problem is sort of a First Amendment one. That is, it sounded to me in the three instances you mentioned—I have no trouble with two of them where you say you don't accept ads for wiretapping and you don't accept ads for electronic eavesdropping. Rather, it is in the debugging one that I have some trouble.

Your assumption, as I listened to it, seemed to be that because some private investigators who advertise debugging services were found through you, or through prosecutions that you observed, to be also capable of or offering services, in fact, to engage in wiretapping and electronic eavesdropping, you therefore were making the judgment that you would not accept any advertisement for debugging.

That troubles me a bit because it is making a judgment that all debugging activity is of that character, or the overwhelming majority of persons who would advertise debugging would be of that character—and also because it denies access to a somewhat important publication for business and commercial purposes.

I wonder how comfortable you feel about saying that all debuggers are buggers in disguise.

MR. CAMING: Professor Westin, first, I do not believe that I said that all debuggers are engaging in improper activity. In fact, I tried to carefully reference the fact that almost all debugging firms are probably highly reputable, and there are other means by which one can obtain the name of a reputable firm.

However, we try in our advertising to afford, within the limits of the publication, a certain amount of protection to our reading public. And we have very limited ways or virtually no way to police these advertisements, as you can appreciate. We have, for example, some 23 million listings in the yellow pages, to give you an idea of the magnitude. Accordingly, since the name or the phrase "debugger" in this selective area has often been a synonym, up to today, for those who are also advertising their capabilities of wiretapping; and since we could not effectively, you might say, engage in policing, we felt that since we were proscribing any wiretapping or eavesdropping at a time when eavesdropping was not illegal, that we would, as the alter ego of both of those, also eliminate any debugging advertising with a full recognition that there is no impropriety suggested towards any particular firm. And I might say up to today the evidence of the number of cases that have been publicly aired, and some prosecutions—a number of which we have been made aware of—in areas such as private detective agencies and debugging firms—have confirmed that at least in some instances there is this impropriety, and it was just a question of how, with the limited resources at our disposal, could we best follow a policy which we had hoped advantages to some slight degree privacy of communications.

MR. WESTIN: I wish I felt a bit more comfortable about the alternative that you mentioned. For instance, if I were a businessman or political leader or involved in civil rights activity and was concerned that my premises were bugged or my telephone was tapped, I might not feel entirely comfortable in marching down to the FBI or the local police department and asking for a list of preferred firms to check out my lines. It exposes my private business to the government. It puts me in a position of wondering whether the local police department will put me in the hands of a former policeman who is now in the business, which is so often the case—a former wireman for the police department will go into the debugging business.

PROFESSOR BLAKEY: Alan, do you think you could call the security officer in the phone company and ask if he could do it—

MR. CAMING: Or Chambers of Commerce or Better Business Bureaus are very pleased to tell those firms that they can to some extent not only

vouch for but police. We have often recommended they consult the Better Business Bureau or Chamber of Commerce in the area.

MR. WESTIN: I have a feeling the first thing the Chamber of Commerce would do would be to look in the yellow pages to see who to recommend. These firms are not like General Motors and General Electric. Most of these firms are one-man or two-person operations. As I think of the Better Business Bureau and the Chamber of Commerce, how do they know what is a reliable firm when these are by the nature of things so relatively small. There are some national firms that do this work, Burns or others that we know of, but I just feel troubled by this.

MR. CAMING: Our experience, Professor Westin, has been up to now this has created no problem at all that we have heard of, except from perhaps a few detective agencies that complained about their ads not being acceptable.

We have had no public concern that they are not getting adequate service.

Normally, this type of service is sought by businessmen who can generally, through a number of sources, obtain a reliable individual or firm.

We are not in a position to indicate to them in this rather difficult area the reliability of every firm. We do not profess to do that. Nor could we fail to ignore—

MR. WESTIN: If I may interrupt you a moment, I think that is my problem with Professor Blakey's suggestion. If you call the security officer at the telephone company, they'd be put in the position of, as it were, assuring the reliability of the firms they recommend or making some claim or disclaimer, and I think the telephone company would probably feel uncomfortable about selecting competitors in the area as to who they would recommend.

PROFESSOR BLAKEY: Oh, they could give you three or four and let you choose.

MR. CAMING: It is a rather difficult decision, Professor Westin, as you can imagine. We do not do this literally or very often. But we were aware from the very outset of the problem, and decided at that time, which is some seven or eight years ago, to go down that route. And our experience generally has been received salutarily. And as I said, it has been reviewed.

MR. WESTIN: Thank you.

MR. HERSHMAN: Just one further question, Mr. Caming.

MR. CAMING: Surely.

MR. HERSHMAN: On Wednesday we had testimony which related some rather serious allegations about employees of Southwestern Bell,

specifically employees in the Security Division of Southwestern Bell.

I know that AT&T has done an internal investigation of those charges, and I wonder if you might for the record tell us what your findings have been.

MR. CAMING: I would be very pleased to.

MR. HERSHMAN: Briefly.

[Laughter.]

MR. CAMING: I am just referring to notes, not to all the content of this.

Let me tell you what our position is on allegations made by the police chief and others in the City of Houston.

It has to be recognized that naturally we have limited resources compared to law enforcement with respect to our ability to thoroughly investigate. We do not have subpoena powers. We do not have access to law enforcement files. But we do have a generally capable group, and we have made a thorough investigation to the extent of our resources as one of the steps.

Now, these investigations were not done by personnel within Texas, but we brought in the Southwestern Bell security chief himself, the general security manager, from St. Louis Headquarters.

In addition, our AT&T Director of Corporate Security made an independent investigation—again within the frame of our capability—and we have very carefully, because of the gravity of the charges, investigated this.

But secondarily, and perhaps of most significance, we have made repeated requests to Chief Carroll Lynn, to the county prosecutor of Harris County, District Attorney Carroll Vance, who coincidentally—and I have some of the newspaper stories here—has asked Mr. Lynn to produce the charges that he made, as to any proof or any name or any indicia of guilt that we could use to further our investigation.

Of course, we were cooperating fully not only with District Attorney Vance, but we have also contacted the United States attorney.

And I'd like to just briefly read—and it is brief—our contact with the Federal Bureau of Investigation whom we have worked with. This is a letter of December 20 of last year, and I will just quote briefly from it:

"We are especially concerned when such charges include the involvement of telephone company personnel. We find it particularly frustrating when we cannot find any basis for these charges. We take the business of protecting the privacy of telephone service very seriously. If you learn of any information whatever concerning any violations by our em-

ployees, we would appreciate hearing from you so we can take proper disciplinary action, including dismissal.

"Furthermore, it is our policy that any violation of Title III be vigorously prosecuted.

"We shall continue to assist you in every respect in this endeavor."

It is signed by the Security Manager, Southwestern Bell in St. Louis, addressed to the Special Agent in Charge, Houston, Texas.

Now, we made a similar request and have spoken several times to Chief Lynn. We have so far received nothing whatsoever—until recently, this past week for the first time, through the kind offices of the House Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the Committee on the Judiciary, we gained access for the first time, not through Mr. Lynn, but through the good graces of Mr. Lehman, the majority counsel, to certain transcripts of officers, several of whom are apparently under indictment, who made certain allegations.

MR. HERSHMAN: The Commission has those transcripts—

MR. CAMING: Pardon me?

MR. HERSHMAN: The Commission has those transcripts available to us.

MR. CAMING: I see. Then that is of particular interest because we had not been able to see this information before, though we had been repeatedly trying to.

We are getting copies of selected pages which refer to the telephone company, and we intend to launch a further and more detailed examination, including an appropriate examination of the offices involved and any leads on employees that may have been involved.

This investigation will be conducted by AT&T under its Director of Corporate Security, at the behest of our higher management. And it will be, of course, with close coordination of the management of Southwestern Bell.

We also learned a tape of a conversation between Chief Lynn and the Southwestern Bell Security Manager at a luncheon was supposedly so garbled as to be unintelligible. We have contacted at my request Mr. Lehman—in fact, I think it was done yesterday formally—and requested that under proper protective custody that that tape be turned over to our Bell Telephone Laboratories who have extremely sophisticated equipment, in an effort to decipher the tape.

We wish to do so because this would permit a determination of the veracity or lack of veracity of the statements made by Chief Lynn with respect to that luncheon, which have been categorically de-

nied by an employee of long standing. And as you can appreciate it, faceless accusations up to now have paralyzed our ability to conclude this phase of our investigation.

Unfortunately, Mr. Lehman has advised—and I state this, I believe, without any breach of confidence—that the tape was returned as too garbled to Mr. Patterson, J. L. Patterson, who is an apparent associate of Chief Lynn, and Mr. Lehman is going to recommend to Mr. Patterson that under proper auspices the tape or a proper copy thereof be turned over to us for resolution of the matter.

No one is more desirous than the Bell System of insuring that any aberrations are rooted out. But also, we cannot act upon questionable allegations made to the newspapers by gentlemen who, when confronted, say, as they said to County Prosecutor Vance, as quoted in the Houston papers which we checked, and he told us that there is no actual proof. We are following this up very closely, and I can assure you that whatever the result is, we shall act appropriately and fully on it.

MR. HERSHMAN: Thank you.

Mr. Feldman.

MR. FELDMAN: Mr. Caming, I'd like to begin with a preliminary question which I think may help the Commission. You used the term both in your statement and your testimony, "Bell System policy." I wonder if you would be able to clarify that term for us without delving into AT&T's corporate structure.

As I understand it, there are 23 operating companies around the country which provide telephone service, and I wonder to what extent those operating companies are permitted to set their own policies in certain areas and to what extent are they bound by policies determined at AT&T's corporate headquarters.

MR. CAMING: Generally speaking, in the area of security matters, the policy of the Bell System is set by the American Telephone and Telegraph Company after appropriate review and concurrence by the associated companies.

For example, by way of graphic example, when Title III was enacted, we required procedures with respect to how to handle court-ordered wiretap requests. The initial procedures were prepared and carefully reviewed at AT&T and approved up to our highest levels of management. They were then presented to the presidents of each company at a joint conference, or I guess in this case they were sent to them after the conference. And their comments were invited and any suggested changes.

They were received and reviewed, and then the final document was established, and it was sent out as Bell System policy.

In the last analysis, AT&T establishes the policy in conjunction with its associated companies and bears the responsibility for it.

MR. FELDMAN: And does that mean that AT&T has enforcement power?

MR. CAMING: In the sense that all the companies of the Bell System are committed to the strongest possible protection of privacy of communication, there has not been any need for enforcement of policy. I might say, parenthetically, that in all but two companies we have the whole controlling interest stockwise, and in those two companies we have a very substantial shareholder interest.

MR. FELDMAN: As an example, you included in your statement here today, and I know in other forums you have stated, it is Bell System policy that your operating companies do not engage in training law enforcement personnel.

MR. CAMING: I do not believe I said that. I believe I said—and I can understand that long statement—that we do not engage in training law enforcement personnel in methods of wiretapping and eavesdropping. I mean this was my reference.

MR. FELDMAN: Does that mean that it is not against—

MR. CAMING: For example, we would train all of our customers, say, in how to use our PBX's—might give them courses in familiarization with our plant equipment, take them through our traffic departments, sometimes perform instructional surveys for them.

In other words, there are a number of services. But we do not train them to be engaged in wiretapping or eavesdropping.

MR. FELDMAN: All right. Let me be more specific.

Are you aware of at least two incidents which occurred in June of 1970 and April of 1971 that have come to the Commission's attention in which representatives of the Chesapeake and Potomac Telephone Company here in Washington apparently held special training schools for agents of a federal law enforcement agency in general telephone theory?

MR. CAMING: Mr. Feldman, it has been a distinct pleasure to deal with you over a period of time, and you were kind enough to bring this to my attention earlier, and I have reviewed that very carefully.

For a period of a couple of years, starting about 1967 or so and terminating about 1970 or '71, a number of government agency personnel—a few of them were in law enforcement—did participate in a plant familiarization course, the type that we would normally give to basic installers, indoctrination and orientation.

Some, I understand, were in law enforcement. Others were from the Department of State, the FAA, the Department of Highways, District of Columbia.

When that program came to the attention of upper management in the C&P Company in late 1970, it was felt that it should be terminated, for two reasons: One, it didn't appear to be part of our basic responsibility to be doing that; and secondly, it was subject to some misconstruction, particularly in view of our strict policy of not training law enforcement. So that the program was terminated.

To my understanding, it was not a program of other than familiarization with general plant theory.

MR. FELDMAN: So that the record is clear—I don't want to leave any impression there is anything illegal about it—

MR. CAMING: I understand you, but our policy was brought out in a letter by our Director of Corporate Security of AT&T that we do not provide any information to law enforcement except with respect to specific court-ordered wiretapping.

With respect to general techniques and methods, we do not design equipment for wiretapping or eavesdropping, nor do we train them nor assist them in effectuating it.

MR. FELDMAN: Thank you.

MR. CAMING: Thank you, kindly.

MR. FELDMAN: I'd like to ask you a number of questions, turning to a different subject, which have to do with the matter of pen registers.

Now, as the staff has traveled around the country speaking with law enforcement officials and others familiar with the court-ordered system, I think it would be safe to say no single subject has caused more confusion than the matter of pen registers.

Let me begin by asking: Is it correct the term "pen registers" is a generic term which describes a number of different devices which do basically different things but may be used for slightly different purposes?

MR. CAMING: That is correct. A pen register is a generic term, if I may just amplify, for the type of equipment that would record the dialed number. So call them dial impulse recorders—there are various models.

MR. FELDMAN: You do not provide that equipment to law enforcement agencies, though.

MR. CAMING: No, we do not.

MR. FELDMAN: That means if a law enforcement agency wants to use that kind of equipment they must secure it on their own?

MR. CAMING: Yes. This is very commonly available commercial equipment.

MR. FELDMAN: Manufactured by different concerns?

MR. CAMING: A large number of different manufacturers, such as Dianetrics, I think is one.

MR. FELDMAN: There are several manufacturers. The equipment manufactured by these different concerns varies in its sophistication and its nature because it may be used for slightly different purposes? Is that also correct?

MR. CAMING: Well, some have greater capabilities than others as far as the amount of paper recording, dial impulses, and numbers.

MR. FELDMAN: Is it correct that some of these devices commonly referred to as pen registers also have built into them the ability to monitor conversations which are occurring on the line to which the device is attached?

MR. CAMING: I beg your pardon? I missed part of that.

MR. FELDMAN: Is it also true that some of these devices at the more sophisticated end of the spectrum also have the capability, perhaps if another set of earphones were to be attached, to monitor conversations which are occurring on that line?

MR. CAMING: Yes, and that is the subject of our concern. It is not so much that they have the capability but all you have to do is insert a jack in a large number of them and attach a tape recorder.

MR. FELDMAN: Or a set of earphones?

MR. CAMING: I am not sure about that aspect without some way of overhearing the voice. But it might just be earphones. But certainly you can, by plugging in, have the capability of overhearing the voice conversation.

MR. FELDMAN: Does the Bell System have a uniform policy—

MR. CAMING: I might say that not all pen registers have that capability. A number of sophisticated models do.

MR. FELDMAN: Does the Bell System have a uniform policy in regard to the nature of legal process which is required before the information which would allow a pen register to be hooked up is provided?

MR. CAMING: Yes. We have very crystal-clear policies which have been reduced to writing.

For example, on April 30, 1975, a communication to all Bell System security managers and also security counsel—and in each company we have a security counsel as a member of the Legal Department of the particular company who comes under my general oversight in this area—restated the recommendation that private-line facilities not be furnished to federal law enforcement authorities acting under non-Title III court orders, for use in connection with a court-authorized pen register.

Cable and pair and multiple record appearance record information are only to be released subject to due process, such as lawful court orders. And we state it's our unequivocal policy to adhere to the fact that in a non-Title III situation, assuming arguing the validity of the use of a pen register by law enforcement authority—very often federal authorities proceed under Rule 41(b) of the Federal Rules of Criminal Procedure—assuming that validity, we feel, first, that as a matter of policy and our concern for providing assistance in only those situations where Title III safeguards are written in, and as prescribed by Congress, or in adequate security situations, that we should not provide a private line which has a potential for other use.

That is our general policy, and one which we have endeavored to adhere to, and we have litigated several times, twice to the Fifth Circuit now.

MR. FELDMAN: But the question is: Exactly what type of process is necessary? I know from experience we have found a variety of different methods by which law enforcement seeks pen register information. Sometimes it is in the form of a subpoena, sometimes in the form of a Rule 41 type search warrant. Other times they go in and get something hybrid in the nature of the Title III. And there is a great deal of confusion.

MR. CAMING: That is one of the points that is, of course, confusing to us, because we feel that it is for the Congress to determine this question as to the extent to which a pen register can be used in law enforcement activity. And we take no position against such use and recognize it as a useful tool, both for strategic information and perhaps obtaining probable cause for ensuing Title III orders.

The only question is: Should we voluntarily, with also incipient civil liability—and we have been sued in a number of cases on other matters—undertake to provide, in addition to cable and pair, which we do have to provide as business record information, but we only provide it under subpoena duces tecum of a court or grand jury—we do not recognize an administrative summons—in addition to that whether we should also provide a special private line, not the one that you would get if you took an office and wanted to interconnect to your office down at headquarters, where you would go in and get a normal private line or normal telephone service—but one that goes to the terminal.

And it is a difficult decision but our overriding concern is for privacy of communications and the fact that if we assisted the federal authorities we would be subjected to the same requirements from every local and state judge throughout this country.

And, accordingly, we felt that our responsibility as a regulated common carrier dictated that we act conservatively in this area as we do in so many others.

MR. FELDMAN: Thank you.

I'd like to explore several other areas where there is some confusion, and perhaps you can assist the Commission in clearing it up.

You include in your statement some information about toll revenues, toll bill information.

MR. CAMING: Yes.

MR. FELDMAN: The only question I have in this area is this: In one locality on the West Coast the staff has been advised by law enforcement officials that subscribers are given the option of asking the telephone company that their toll records not be retained except for the very short period of time for which they are necessary after billings—I guess something less than 30 days. And this has, at least in one instance that the staff is aware of, thwarted law enforcement efforts to subpoena these toll records.

Is this a policy in any of your operating companies?

MR. CAMING: I am afraid, although I am not certain of the company and even whether it is a Bell System company—it appears to contravene the requirements of the Federal Communications Commission System of Accounting which requires us to retain, as a minimum, all toll billing records for a period of six months. And we uniformly do it throughout the Bell System. On occasion, we have kept them longer, if, for example, law enforcement has asked in a specific case that we retain them. But to my knowledge, we do not destroy any prior thereto. You would offend federal regulations and presumably intrastate regulatory recommendations.

MR. FELDMAN: Thank you.

On the question of subscriber information, where they have a wiretap, a pen register or similar device and keep on a day-to-day basis a list of every outgoing call made—they have nothing other than the telephone number—does the Bell System have a policy on providing subscriber information to law enforcement officials based on those kinds of records?

MR. CAMING: If I understand you correctly, when law enforcement is acting under a Title III court order and presumably we are providing information and facilities as provided by the court directive, part of that would be such business records relating to the subject of the order as law enforcement would require, including the names and addresses of any telephone numbers identified.

That would be part of what has been rather uniformly construed, in the sense that it hasn't been

challenged in the court, the provision of information in connection with facilitating wiretaps.

MR. FELDMAN: The last area in this phase that I'd like to ask you about is something which is known most commonly as a call forwarding system, which I understand is a relatively recent development of the Bell System. As I understand it, it is a service which you provide to subscribers by which a person who desires to be able to forward calls or receive calls at a location other than his home or office, with the proper equipment can simply dial on his home telephone the number to which he wishes calls forwarded, and then through computerized equipment in your central office any numbers which ordinarily would be coming in to his telephone would be automatically diverted to the number that he has requested.

Now, the concern that we have found among law enforcement officials—and they may not be correct in their understanding of the technical aspects of it—but their concern is that if this were put on a telephone and a Title III court-ordered wiretap was placed on that phone, that if the individual diverted his call to some other number, that would circumvent the wiretap. Is that correct?

MR. CAMING: Yes. And if I may just very briefly explain, call forwarding is a feature a subscriber may obtain as an option. It is not available as yet throughout the United States but is in a number of locations.

When call forwarding is provided, it is usually in conjunction with an electronic switching system office, E.S.S. office, which is more computer controlled.

Now, the call forwarding feature is in the computer, and the subscriber has the capability, when he is leaving, to forward his calls by certain dialing arrangements to another telephone number.

When he does that—and let's say it is my number and I am going to visit you, Mr. Feldman. I would dial your number and, in effect, tell the computer, "Any calls to my number are to be diverted."

Now, they will come into the E.S.S. central office and will immediately go to you. They won't go to my phone. So that if you were overhearing calls on my telephone, you would not be hearing any calls coming in during that period.

The party could still, if anyone was at home, make outgoing calls.

In that case, we do provide certain assistance to law enforcement when they request it. We don't automatically know—we don't have any way of knowing without a laborious process what number it has been forwarded to. But we can tell law enforcement whether or not there is a call forwarding feature which the subscriber has. And then the law en-

forcement could request us, by serving an appropriate order or subpoena, to advise them at that time what number that call has been diverted to.

This would require us to literally search the computer with a very specialized craftsman, who would go into the "call" store area of the computer and search, and it could take from a few minutes up to 35, 40 minutes from experience, and the employee can find that particular number. And then we would be glad to provide that information under proper auspices.

Now, I think it is fair to say that we would not be in a position to assist, without a further court order, on providing assistance to the number to which the call has been diverted. The reason for that is that this would necessitate all calls to that number, not only by the person who diverted calls there, but everybody else's calls to that number would also be intercepted, and we would have to have a court order to relate to that.

But should we get a court order that would relate to that particular number, we would accord the same assistance as we would to the so-called home number.

Now, the way those numbers are changed might be of interest to you very briefly.

The party must come back to his home to change that call diversion—or someone else at his home could do that. And when he does that, that erases the call. We don't have a record.

In other words, if you ask me: What were all the numbers called within the past three months that Professor Blakey's phone may have diverted, we could not tell you. At most we could tell you perhaps one back, but the others are automatically erased.

Does that answer your question?

MR. FELDMAN: Yes, it does. The concern at this moment is that as a practical matter law enforcement would have a difficult time securing court orders quickly enough to overcome that difficulty, particularly if the individual was frequently changing the number to which the calls were to be diverted, which I guess someone probably would if they were attempting to circumvent a wiretap.

PROFESSOR BLAKEY: We will take a five-minute break at this time.

[Whereupon, a short recess was taken.]

MR. STEIN: Mr. Chairman, may I interject for a couple of questions?

MR. BLAKEY: Mr. Stein.

MR. STEIN: Chief Andersen of our Commission, unfortunately, had to leave early and asked me to ask these questions on his behalf. They concern the telephone company's cooperation with local law enforcement authorities on court-ordered wiretaps.

We found some degree of variance in the Bell System as to the degree of cooperation in furnishing leased lines, for instance, between New York and New Jersey. New Jersey authorities find their cooperation from the telephone company much better than, say, New York City authorities, although both of them have court orders.

Can you explain the variance in telephone company policy there?

MR. CAMING: Yes, Mr. Stein.

I might say, by the way, that I have personally heard nothing but the utmost commendation about cooperation in New York. Mr. Miller, the Security Manager, has been very highly regarded by both local and federal authorities.

I think it is just a question of perhaps definition as to what we are talking about by degree of cooperation.

Both companies accord the same cooperation, and the methods employed may vary with the individuals, but not in the approach to the subject. The idea is to do everything possible to effectuate a particular wiretap as effectively and as swiftly as possible.

To give you an example, when law enforcement might advise in New York City, just taking this hypothetically, that they would require a private line—the federal authorities—between Point A and Point B roughly, that they anticipate getting a court order, say, within six or seven days, New York Telephone Company would when provided the location of the listening posts in the suspect's terminal begin the necessary preliminary steps.

As you know, these private lines very often, particularly when they go through more than one central office, have to be specially engineered. You may need a wider gauge cable. You may need what they call long-line sets to make sure the transmission is maintained at a proper quality so the intersection of the line does not indicate an aberration to the parties to the conversation.

All these measures and special engineering may take, say, a week to do.

New York Telephone will normally initiate such measures and when the order comes in they will either go along or, if they have finished it, be prepared to activate the line and turn it over to the authorities as soon as possible. So they do everything possible.

A lot, too, depends on the facilities, the geography, whether you are dealing with Summit, New Jersey, where I live, or New York City, where you have quite a few different problems.

MR. STEIN: The issue seems to be on private-line channels which are much more difficult to get for New York City police officers than for New Jer-

sey officials, so that New York officers sit in basements, whereas New Jersey officers can get the wires into their normal offices.

MR. CAMING: To a degree there it depends on facilities. We endeavor to make it uniform, and if there are any special problems in a particular area, normally they can be ironed out with the particular local authorities. And, of course, we are always pleased to entertain any problem areas that any authorities might present.

I, for example, know that our Director of Corporate Security maintains very close contact with all the companies. So if there is any way we can review a situation with a particular company, we are always pleased to do so.

MR. STEIN: Why the distinction between furnishing private-line channels and furnishing of all other sorts of information, such as cables and pairs?

MR. CAMING: It is our policy to provide that information necessary to effectuate the wiretap, but to provide the minimum assistance. And unless it is an area like the federal area, and the District of Columbia and eight states have a directive provision, we do not provide a private line in the first instance. And we only provide line access information, and then only such additional assistance as a particular case may necessitate to effectuate the specific wiretap.

And the reason, in part, is that it is the prerogative of the Congress or the state legislature to determine the degree of assistance they wish provided. And in a number of states they have rejected the so-called court-directive provision and refused to put it in their law.

Now, we do have two policies. I hope you will understand. That is set forth in our statement. When there is a court directive, we do provide a private line in the first instance. When there is not, we provide only line access information.

And there, again, there is a question of the degree of cooperation necessary to effectuate the particular tap.

We do ensure in each case that sufficient cooperation is extended—but no more. And we do not do it on the basis of convenience or law enforcement, but rather upon our top management tripartite decision—legal, security, and operations—as to whether the type of facility and operations require more assistance.

But when there is a court directive—New Jersey has a court directive provision pending. I thought the law had been passed but it has been recalled.

When that law is obtained, we will then provide assistance as above described when and if we receive a state court “directive”—now, New York

rejected several times, although it has been before their legislature, the court-directive provision.

So we cannot, we feel, in a sense go beyond what the state legislature wishes to be accorded to its law enforcement officers.

MR. STEIN: But the purpose of effectuating the wiretap makes little difference after they are furnished these private-line channels. The difference is the comfort and the ability of the police to check themselves on the ability to wiretap. They can't wiretap from basements. But why this distinction as to furnishing private lines?

MR. CAMING: Well, our point is to provide the minimum assistance, in view of the fact that our basic responsibility is not to be in law enforcement but to be common carriers responsible for provision of service and privacy of service. We have a very dual responsibility. And we feel we should do what is necessary in the concept of the legislature to carry out the legislative mandate. But we are very conservative in going beyond that.

But we do in each case take all measures necessary to ensure that the particular wiretap is effectuated.

MR. WESTIN: May I ask a question about that, please, on the same line. Suppose that Congress or the states in its legislation were to provide as a requirement that the telephone company, when a court order was obtained, provide a direct line; that it be to a secured place; and that all listening on the telephone that was not conducted at the central place would be unlawful, thus providing an opportunity for centralized listening, perhaps providing more control over amateur, illegal, beyond-the-border-of-authority, wiretapping.

Would you have a reaction to that as a potential for policing lawful court-ordered wiretapping more effectively than when it is done in a variety of basements, attics, rented motel rooms, et cetera?

MR. CAMING: Professor Westin, I feel that law enforcement generally in our experience has scrupulously observed the requirements of Title III, and that probably would make little difference. I think the problem of illegal wiretapping is not in any sense interfacing with where the wiretapping takes place, but the character of the people who are doing it.

And I submit it would be even easier and perhaps more dangerous to have a centralized position which could, in a certain sense, almost have unrestricted access to the lines of a city.

In a particular wiretap, we provide certain minimal assistance, but at the actual access to the premises where it is done, the actual wiretap itself is done by law enforcement.

And I think the idea is well-taken that if you did have a centralized place you might be able to have closer supervision. We, for example, find that in service observing locations we foster and favor centralization. On the other hand, many people would be concerned about the creation of a wiretap center that dominates the city. You have seen that in newspaper articles.

MR. WESTIN: I have had some experiences as you have with the descriptions perhaps being broader than they may have been or than the situation would really justify. Have you ever thought about why creating a center would, not in terms of newspaper stories but in fact, create great problems? That is, if every connection that went into the center had to be verified and if at any point on a sporadic check basis you would be able to ascertain that at the center only authorized court-ordered taps were being fed in, you don't really have the image of a switchboard plugging in anywhere in a city.

MR. CAMING: That is true, but we do not police the wiretaps, as you can appreciate. We provide the facilities. The actual tapping and supervision of tapping is done under the auspices of the court. We do not access their premises. So we would actually not know the uses to which the equipment was put once it was in. All we would know, of course—and we know that to the same extent wherever the location—we assure ourselves that it is a court order valid on its face. And what happens to it and whether it is abused or not, or transcends the bounds, is something we do not know, since that is the province of the courts.

MR. WESTIN: What I am trying to suggest is just for the purpose of exploration—and I am not committed to this as a suggestion, but it seems to me something that we as a Commission ought to be discussing at a hearing like this with a telephone company. As it is now, law enforcement officials go into the basement, say, of an apartment building or office building. You give them the pair numbers, and what they do down there you don't know. In much popular writing, the idea is in the wee hours of the morning when things get boring, some law enforcement officials might listen to some other apartment, some other office. There is the sense that once they are there at the box where all the pairs come, nobody is watching to see what they do.

Supposing for the minute that takes place—how much I am not trying to estimate here—the alternative I am raising with you is that if you gave one connection from the pair that was given court-ordered authority to eavesdrop into a listening post, wouldn't you be able to insure only that line was

the line being listened to because there would be no other pairs given access to law enforcement, and wouldn't that provide far greater security against random listening to unauthorized telephones than the present highly decentralized, unsupervised, unmonitored technique of electronic eavesdropping?

MR. CAMING: I would certainly say that if we provided facilities to a centralized listening post, we'll say, for each city—and I presume for each authority within the city, since you have a number of law enforcement authorities—that from our standpoint it would certainly be no more difficult. And if, in the viewpoint of the legislature and the Commission, that was a desirable location from which to have law enforcement operate, I would preliminarily, subject to any operating considerations of our people—I would see no objection to our providing lines to that location.

We provide facilities to whatever location is designated. And if, in the wisdom of the Commission and the Congress it appeared to be more appropriate on balance in their experience, we would see no objection.

MR. WESTIN: I would appreciate it, after having a chance to reflect on it and perhaps talk it over with others in the telephone company, if you wanted to amplify your reaction to this you could submit something to us. Because it seems to me when you started out you identified law enforcement sites wherever located, not supervised, as broadly the right way to go. Then as our discussion has gone on—

MR. CAMING: We would still not supervise in any respect. What I am saying to you—

MR. WESTIN: By supervision all I mean is what I said before, that you'd put only the one line that was court-identified into that room.

MR. CAMING: This, of course, is a question of the facilities, too. I am assuming that if it was the desire of the Congress—of course, it could be more expensive for law enforcement, and that would be for them to determine. For example, if everything ran to one point, it might be more expensive facilitywise than being very close to the line of operation, for two reasons: One, the length of the facility and the special engineering might require us to impose larger charges in a particular case. That could, of course, balance out on an average.

Secondly, at times they may want the listening post for other purposes like physical surveillance, in closer proximity.

But certainly we could provide those facilities, as we do now, to any central point. It really makes no difference to us. The question of policing each case is done by us to the extent of very carefully determining the validity of the order, and of insuring that

our facilities comport with the order. Beyond that, it is the province of the court.

So I could not pass upon the question as to whether one site is more desirable than the other. It is really between law enforcement and the legislative authorities.

MR. WESTIN: Thank you.

MR. STEIN: We have noted in our travels the degree of willingness among subsidiary companies of the Bell System to provide those private-line channels does vary, and also, for what it's worth to you, some of your rival companies like Rochester Telephone Company have no hesitation, despite the lack of directive of New York State, of providing these facilities to the police.

A related issue that Chief Andersen wanted to raise was the telephone company definition of what constitutes a court order valid on its face. We have heard from an assistant D.A. in Arizona and we know it is also true in the State of Colorado that telephone company practice there is to scrutinize a signed order that has already been scrutinized by the D.A. and signed by a judge of competent jurisdiction. Nevertheless, it is scrutinized and sometimes held up or refused to be acted upon by the telephone company.

MR. CAMING: I am familiar with that episode.

What we do is recognize what is the desire of the Congress and the states that law enforcement act only under orders that are valid. And this order is not only protective to us and the public but also to law enforcement because a prosecution predicated upon a faulty order would be deficient.

Accordingly, in the one case or two to which you have reference, the orders were actually defective on their face and all that was pointed out was that the order needed correction, and it was corrected and assistance was promptly provided.

We do scrutinize it because we feel it is the intent of the Congress and of the state legislatures that we do not cooperate except when the order is valid on its face. We do not endeavor to go behind the order. We never ask about it afterwards for the supporting evidence. But if an order is void on its face, I do not see how we can cooperate.

MR. STEIN: The question was the interpretation of the state law by which the D.A. and the judge's interpretation of the state law varied from the telephone companies—at least in the Arizona situation.

MR. CAMING: In that instance, I am certain the judge would have apprised us of the propriety of the order. And I do not fault our people if there is any doubt of having our lawyers request the court to review the order if they have an objection. I think it is for the benefit of the public and for the

benefit of law enforcement to insure that the orders appear valid.

If there is a defect question of that type, which may be an erroneous interpretation on our part, once it is clarified, it is clarified in perpetuity. So this problem you referred to, once ironed out, was no longer a problem.

But we do try to accord the utmost accommodation to law enforcement and act as expeditiously as possible whenever we are confronted with a situation of this type.

MR. STEIN: Thank you.

MR. FELDMAN: Mr. Caming, the rest of my questions have to do with the subject of electronic toll fraud, and we have three other witnesses who are going to add some testimony to that as well. So I think in view of Professor Blakey's requirement that the next witness testify—

PROFESSOR BLAKEY: The procedure we will follow is when Mr. Caming is finished, at this point we will temporarily relieve him and put on Mr. Linehan, and when he is finished we will bring up the other gentlemen to discuss the general subject of monitoring and ask Mr. Caming to come back. But I understand Commissioner Westin has one or two questions of Mr. Caming.

MR. WESTIN: My questions do not relate to the matters that are going to be taken up by other witnesses. One is a question of legislative amendment.

Do you feel that Title III needs any amendments in order to specifically protect the privacy of data communication on telephone lines? This is an area I worked in in the computer privacy field, and it can be argued that apart from the protection of business proprietary information and fraud suits, we lack in the United States a generalized protection by statute of privacy of confidential personal information—not by voice—when it travels across the telephone lines, and that we have some gap here in terms of what kind of federal express protection of such data, criminal penalties about attempting to intrude into the movement of confidential personal data by leased-line data communication, and so on.

Have you thought about that and do you have any recommendations to give us?

MR. CAMING: Yes, I have given a lot of thought to this subject, and this is one Professor Blakey and I have discussed in the past, and I have expressed concern as to the interpretation of the phrase "aural acquisition."

There are two approaches—and I say this because we have the current statute which we are living with.

It could be argued that aural acquisition means the acquisition of the electric signals going over a wire communication.

It must be recognized that voice and data are really electric signals demodulated to, in one case, the level of frequency that we can recognize by the ear, and in the case of data, that can be seized upon by the computer and acted upon.

And in that sense, the aural acquisition is the same. You are not taking voice or you are not taking data. You are taking electric signals, and then you have to convert them and process them.

So in that sense, I would hope that the present prohibitions of Title III would extend to that.

On the other hand, search of the legislative history reveals little or no real concentration in this area. Rather, they were talking about interception of voice conversations. And my concerns, which I mentioned to Mr. Reynolds, of the Department of Justice, as to whether he had any suggestions—and, of course, Mr. Reynolds is speaking only in a certain area of the department—this is one of the concerns, because not only in private business but much of the criminal justice network is data. And if criminals could, with impunity, intercept, it would certainly be a state of affairs that would be alarming.

In addition, it would raise questions of industrial privacy. And, of course, today the computer is vital to segments of government and industry.

So my answer is: As a lawyer faced with the existing statute, I would firmly state without equivocation that a strong argument can well be made that Title III applies. But I am concerned as to whether that argument would be acceptable to a court after really scrutinizing the congressional background.

MR. WESTIN: Without knowing what our Commission might conclude as a corporate body, I think we should seriously consider an amendment that would extend the protection of private communication by data through congressional action.

In that regard, would you be willing to put your mind to drafting for us, as a suggested line of approach, what kind of provisions you think might be considered by this Commission for recommendation to Congress that would extend the proper kind of protection to data communication?

For example, you may be familiar with the fact that Sweden passed a data protection act in 1973, and protection is not given to just the storage of data in computer banks but also the transmission. It might be worth looking at that but I am sure you might have other ideas than just imitating the Swedish model. If you could write a nice, strong amendment that would give protection—I am not so much concerned with the industrial and proprietary information, but so much of the personal data dealing with people's medical records, dealing with information about welfare and other

non-law enforcement information, is increasingly being transmitted by data communication, and there are high vulnerabilities for extraordinarily important private personal information collected by government, and in the credit and insurance fields collected by private industry.

And I would welcome having your thoughts on this so we can consider it when we turn to possible amendments.

MR. CAMING: I will be very pleased to endeavor to put something on paper.

MR. WESTIN: Thank you. I wonder if you could say a word on the subject I don't think your statement addressed, the question of the way the telephone answering service, as it has developed over the last few years, may open some vulnerabilities for private communication.

What I have in mind is this. We have had it described to us in several communications to the Commission that the creation of telephone answering services means there are now people in each city who are able to pick up on individual telephones of persons who subscribe to their services after the required number of rings and answer the telephone; and that this is accomplished through means that I am sure you could describe more specifically, of a connection in the telephone machinery itself, a link between the telephone number of a subscriber and the telephone answering service.

That raises in my mind the question of who is now engaging in the business of telephone answering services. What verification is made of the fact that my telephone is now connected to a telephone answering service? And what kind of abuses may be taking place?

I have had brought to my attention accusations that because these are relatively small-scale operations, not national companies that seem to be doing it, a good way of conducting business espionage is to form your own telephone answering service or corrupt one from inside and get the ability to listen in to the telephone conversations of persons who use telephone subscription services.

I wonder if you could say a word about this in general and give us your thinking on it?

MR. CAMING: We are somewhat familiar with the problem because it was voiced, if I remember, during the hearings before Senator Long's committee back in the mid-'60's—the telephone answering service. If my memory is right, a locksmith from the Washington, D.C., area testified on that very subject.

We have a procedure which hopefully eliminates much of that danger, which is uniformly applied throughout the system.

We do not provide telephone answering hook-ups, which are in effect an extension but off-premises, just as you would have in your house, but it is theoretically extended to the Telephone Answering Service Bureau, except as follows: we require the express consent of the subscriber before we will act upon any such request and make the installation.

MR. WESTIN: How is the express consent acquired?

MR. CAMING: In writing—by the subscriber, authorizing us to give the telephone answering service physical access to his line for the purpose of answering the phone.

MR. WESTIN: Do you have a verification procedure to see whether the signature on a piece of paper is, in fact, that of the person who is subscriber to the telephone?

MR. CAMING: We do have verification procedures.

MR. WESTIN: For example, would you call the telephone?

MR. CAMING: We do not take it over the telephone. We require written consent. We usually contact the subscriber who desires the services and inquire from him, and ask him to send in—

MR. WESTIN: Do you do this by going personally to the subscriber with a representative of the telephone company and talking directly to the representative or the subscriber? Or is this done by receiving a sheet of paper, a form that has been signed at the bottom, and calling that number and saying, "We have received this number. Are you Mr. Jones of 2222 North Avenue, and did you sign this?"

How do you verify it?

MR. CAMING: Normally, we would verify it by getting a request orally or in writing, first from the telephone answering service, to provide this. And I would have to recheck this and any of my remarks would be subject to modification.

But I believe that we then verify it with the subscriber himself.

Now, if the telephone answering service brings in the subscriber's request—whether we'd go through a further verification procedure in the apparent absence of any irregularity would depend on the circumstances. But we do have established verification procedures. And we are careful because we have recognized, particularly since Senator Long's investigation, the problem. And we look at this very carefully and attempt to police it.

MR. WESTIN: On the other hand, do you have any procedure for investigating a telephone answering service? Can anybody come to you and say, "I am the Ace Telephone Answering Company and we are now in the business of picking up"—

MR. CAMING: We would assure ourselves that it is a legitimate concern, but what it does besides telephone answering would be difficult for us to do. Once the subscriber has consented and it is verified, the telephone answering service, absent any proof of irregularity, would be assumed to be reputable—just as any of our other customers would be. It would be very difficult for us to endeavor to investigate.

I might point out that when the telephone answering service intercepts, it does not have the capability of overhearing silently, as I understand it. In other words, suppose you were on the line. The telephone answering service could not silently get on and listen to your conversation even if you were subjected to their service. And if you answer the phone first, I think you disconnect the service so even the potential for overhearing is omitted.

MR. WESTIN: That was not my understanding, but I would appreciate your verifying that statement.

MR. CAMING: As soon as we have the transcript on this, I will review this with our people in Commercial, and I am sure that anything that more accurately reflects our practices will be brought to the full attention of the Commission.

MR. WESTIN: Thank you.

PROFESSOR BLAKEY: I have only one further question at this time. I wonder if you would review for the Commission briefly the development and present status of the phone company's policy on what information it provides to a subscriber where, having been asked to check the line, it determines that a device which is known to have an outstanding court order is present.

MR. CAMING: In other words, a non-court-ordered device?

PROFESSOR BLAKEY: No. My question is, say a member of organized crime requests the phone company to check his phone to see if there is a wiretap on it. You check it and, lo and behold, the Federal Bureau of Investigation is there with a court order. What do you tell the member of organized crime?

MR. CAMING: Our practice generally—

PROFESSOR BLAKEY: As you well know, Mr. Caming, I know the answer to that question. What I really want to get in the record is the development as well as the present status of the policy.

MR. CAMING: I'd be very pleased to initiate this conversation.

It is our general and recommended practice that when we find a device, whether legal or illegal—legal being under court order and we are aware of it—that we would notify the customer that we have found a device—we use that term without

characterization. And if he has any questions whatsoever, go to local law enforcement, or go to law enforcement.

We use the generic term "a device" in order not to disclose what it might be.

Second, there are two companies at present that have an express policy, one by statute, Minnesota, and New Jersey by company practice, of advising the customer that, "We will be pleased to check your line, and if we find an unauthorized device we will advise you." And in that case, if they find an authorized device, they report back to the customer, "We have checked your line and found no unauthorized device."

And if the customer asks, as is probably his wont, "What about an authorized device?" we just state, "We do not disclose that information. However, Title III provides that the court issuing any lawful court order is required by law within 90 days after termination of the order, unless it is postponed for good cause, to advise you, and so you will be advised if there is such."

Now, there have also been some cases where we have received in other states court orders directing us not to disclose the presence of a device. In such cases, we have adhered to that order.

That has generally been our practice.

PROFESSOR BLAKEY: And what do you tell the subscriber? We have a court order that tells us not to tell you anything?

MR. CAMING: No, in that case we go into what is known as the unauthorized device approach. We will just tell the subscriber, "We will check your line, and if we find an unauthorized device, we will let you know."

PROFESSOR BLAKEY: Was there a period of time in which the general policy of the phone company was to make the, "we found no unauthorized device" statement?

MR. CAMING: You mean the so-called New Jersey approach?

PROFESSOR BLAKEY: Yes, sir.

MR. CAMING: No, I don't think there was ever a time when that was a general policy. It was a question for a period at the outset of Title III as to what approach should be used.

PROFESSOR BLAKEY: What was the experience with the initial statement to the subscriber that, "there are no unauthorized devices?"

MR. CAMING: That would take us up to today. First of all, two things have to be borne in mind.

First, we have found virtually no lawful devices over the years. We have found a few but virtually none. Out of the 1400 you could probably count a handful.

Second, members of organized crime, for some reason which is probably well-known to us, do not come to us and ask us to check—with rare exceptions. There may be an instance where they may discover a device and then ask. We had one recently in an eastern state where they called the telephone company, and a craftsman came out and the subscriber said, "What is that?" And "that" happened to be a device on his set.

And he was interested in what we would do with it, and we said, "We are just going to turn it over to law enforcement. If you have any questions about it, ask them. We don't know what it is."

We didn't, at the time.

The only point I must bring to the Commission's attention—two points.

We are very troubled by this question, as you can appreciate, because the last thing we want to do is in any sense undermine the lawful device situation. But we have some 10,000 or more requests a year. There are only a handful of devices found by each company. You tell the others, "We haven't found an unauthorized device," and they get all upset and they say, "What about an authorized device?"

And we say, "We can't tell you about this."

And they all go away saying, "Aha, there is an authorized device on our line."

And it has been our experience that this so often happens, and mainly these are innocent people getting very, very upset.

PROFESSOR BLAKEY: Would you ever tell law enforcement to remove it and, having removed it, go back and tell the subscriber, "There is no device on your line?"

MR. CAMING: At one point in a number of companies they did use that route. The one difficulty we found with that is it raised questions as to what our credibility would be when coming before the National Wiretap Commission or Congress or the state legislature and our subscribers as to whether or not this would be thought to be deception if the day after it was removed law enforcement put it back on again, and then it came out in a prosecution and the thing would be labeled as deception by the telephone company.

We feel the one thing we do not want to do and that we cannot do in good faith to our customers is lie.

And the statute does not prohibit disclosure of a device. If it did, then we could point to the statute and say, "That is the situation," and Congress would have to weigh that against the fact that a great many people are going to get awfully upset innocently.

And we have had the amusing situation where courts have said to us, "Don't lie to the customer, but don't tell them there is a device on the line."

And we said, "Well, splendid. Would you like to talk to them? Because we haven't figured out that third route."

PROFESSOR BLAKEY: What we obviously need at this point is a Jesuit scholar.

MR. WESTIN: The trouble is the Nixon Administration has made "inoperative" such a bad term. You could go behind that and suggest the statement may or may not be true. It is operative for a certain period of time and inoperative as of a certain date.

MR. CAMING: Yes. Well, we have thought, for example, of a number of things. In fact, I have explored it with law enforcement authorities, and the Department of Justice, and importuned them to come up with any better method, and they themselves have recognized that this is a Gordian knot.

PROFESSOR BLAKEY: Thank you, Mr. Caming.

I wonder if you could step down for a short period while Mr. Linehan testifies.

[Whereupon, Mr. Caming was temporarily excused.]

[The prepared statement of Mr. Caming and additional materials follow.]

STATEMENT OF H. W. WILLIAM CAMING,
ATTORNEY, AMERICAN TELEPHONE AND TELEGRAPH
COMPANY

I am H. W. William Caming, Attorney in the General Departments of American Telephone and Telegraph Company. My areas of primary responsibility have since 1965 included, from a legal standpoint, oversight of matters pertaining to industrial security and privacy as they affect the Bell System.

I wish to thank the Commission for the opportunity to present the views of the Bell System on privacy of communications and delineate our policies, practices and experiences with respect to electronic surveillance, principally in the area of wiretapping, the disclosure of toll billing record information, and electronic toll fraud.

I

At the outset, I wish to stress the singular importance the Bell System has always placed upon preserving the privacy of telephone communications. Such privacy is a basic concept in our business. We believe that our customers have an inherent right to feel that they can use the telephone with the same degree of privacy they enjoy when talking face to face. Any undermining of this confidence would seriously impair the usefulness and value of telephone communications.

Over the years, the Bell System has repeatedly urged that full protection be accorded to its customers' privacy, and we have consistently endorsed legislation that would make wiretapping as such illegal. In 1966 and again in 1967, we testified to this effect before the Senate Subcommittee on Administrative Practice and Procedure during its consideration of the Federal Omnibus Crime Control and Safe Streets Bill. We said we strongly opposed any invasion of the privacy of communications by wiretapping and accordingly welcomed Federal and State legislation which would strengthen such privacy. This is still of course our position, one which we have reiterated in recent years in appearances, among others, before various subcommittees of the Congress.

We believe that the Federal Omnibus Crime Control Act has contributed significantly to protecting privacy by, among others, clarifying existing law and proscribing under pain of heavy criminal penalty any unauthorized interception or disclosure or use of a wire communication.

During our Congressional testimony, we have said too that we recognize that national security and organized racketeering are matters of grave concern to the government and to all of us as responsible citizens. The extent to which privacy of communications should yield and where the line between privacy and police powers should be drawn in the public interest are matters of national public policy, to be determined by the Congress upon a proper balancing of the individual and societal considerations.

For more than three decades, it has been Bell System policy to refuse to accept in the Yellow Pages of its telephone directories advertisements by private detective agencies and others, stating or implying that the services being offered include the use of wiretapping. In December 1966, during Congressional consideration of the Federal Omnibus Crime Control Act's Title III proscriptions against unauthorized interceptions, this longstanding policy was expanded to prohibit too the acceptance of eavesdropping copy. This standard, adopted by all Bell System Companies, was interpreted from the outset to make equally unacceptable so-called debugging advertising (*i.e.*, advertising stating or implying electronic devices or services will be provided for the detection and removal of wiretaps and eavesdropping "bugs"), on the theory that those who can debug also possess the capability to bug and wiretap.

Our Companies continually review their Yellow Pages in an endeavor to ensure all unacceptable copy is removed, either by satisfactory rewording or deletion of the offending copy. New advertising is subject to similar scrutiny. The scope of this undertaking becomes apparent from the fact that there are approximately 2,300 Yellow Pages telephone directories, containing some 23,000,000 advertisements and listings.

The removal of unacceptable copy is a never-ending task, since many such advertisements are revised, and new ones appear, in each issue. We believe, however, that we have done a creditable job in this area, and we intend to continue such rigid policing as contributive to maximizing privacy of communications.

It may help place matters in perspective if we provide a brief insight into the magnitude of telephone calling that occurs in this country in a single year. During the calendar year 1974, for example, there were approximately 144 million telephones (including extensions) in use in the United States, from which more than 200 billion calls were completed.

From the time our business began almost 100 years ago, the American public has understood that their telephone service was being personally furnished by switchboard operators, telephone installers and central office repairmen who, in the performance of their duties of completing calls, installing phones and maintaining equipment, must of necessity have access to customers' lines to carry out their normal job functions. We have always recognized this and have worked hard and effectively to ensure that unwarranted intrusions on customers' telephone conversations do not occur. We are confident that we have done and are doing an excellent job in preserving privacy in telephone communication.

The advance of telephone technology has in itself produced an increasing measure of protection for telephone users. Today, the vast majority of calls are dialed by the customer, without the assistance of an operator. This has greatly minimized the opportunities for intrusions on privacy. In addition, some 90 percent of our customers now have one-party telephone service, and the proportion of such individual lines is growing steadily. Direct inward dialing to PBX extensions, automatic testing equipment, and the extension of direct distance dialing to person-to-person, collect and credit card calls and to long distance calls from coin box telephones further contribute to telephone privacy.

Beyond this, all Bell System Companies conduct a vigorous program to ensure every reasonable precaution is taken to preserve privacy of communications through physical protection of telephone plant and thorough instruction of employees.

Our employees are selected, trained, and supervised with care. They are regularly reminded that, as a basic condition of employment, they must strictly adhere to Company rules and applicable laws against unauthorized interception or disclosure of customers' conversations. All employees are required to read a booklet describing in unmistakable terms what is expected of them in the area of secrecy of communications. Violations can lead, and indeed have led, to discharge.

Any allegation of illegal activity leveled against any of our employees—or any evidence thereof, whether uncovered in our day-to-day operations or brought to our attention by any outside sources—is promptly and thoroughly investigated and, if the facts so warrant, appropriate disciplinary and prosecutory action is taken. Additionally, it is longstanding Bell System policy to cooperate fully with law enforcement authorities and other duly authorized government agencies in their investigations of alleged or suspected illegal activity by our employees.

In regard to our operating plant, all of our premises housing central offices, equipment and wiring and the plant records of our facilities, including those serving each customer, are at all times kept locked or supervised by responsible management personnel, to deny unauthorized persons access thereto or specific knowledge thereof. We have some 90,000 people whose daily work assignments are in the outside plant. They are constantly alert for unauthorized connections or indications that telephone terminals or equipment have been tampered with. Telephone cables are protected against intrusion. They are fully sealed and generally filled with gas; any break in the cable sheath reduces the gas pressure and activates an alarm.

With these measures and many others, we maintain security at a high level. We are, of course, concerned that as a result of technological developments, clandestine electronic monitoring of telephone lines by outsiders can be done today in a much more sophisticated manner than has been heretofore possible. Devices, for example, can now pick up conversations without being physically connected to telephone lines. These devices must, however, generally be in close proximity to a telephone line, and our personnel in their day-to-day work assignments are alert for signs of this type of wiretapping too. Every indication of irregularity is promptly and thoroughly investigated.

Our concern for the privacy of our customers is reflected too in the care with which we investigate any suspicious circumstances and all customer complaints that their lines are being wiretapped. Our Companies follow generally similar operating procedures when an employee discovers a wiretap or eavesdropping device on a telephone line. Each Company has established ground rules for the small number of these situations that occur, which take into consideration any local statutory requirements. Most frequently, when our people find improper wiring at a terminal, it is the result either of a record error or failure on the part of our personnel to remove the wires associated with a disconnected telephone. Each of these cases is, however, carefully checked. In those few instances where there is evidence of wiretapping, the employee discovering it is required to inform his supervisor immediately, and a thorough investigation is undertaken in every such case by competent security and plant forces.

In a small number of cases, a customer suspects a wiretap and asks for our assistance. Usually, these requests arise because the customer hears what are to him suspicious noises on his line. Hearing fragments of another conversation due to a defective cable, or tapping noises due to loose connections, or other plant troubles are on occasion mistaken for wiretapping. Each Company has established procedures for handling such requests. Generally, the first step is to have our craftsmen test the

customer's line from the central office. In most instances, these tests will disclose a plant trouble condition. In each such case, the trouble is promptly corrected and the customer informed there was no wiretap.

In cases where no trouble is detected through testing the customer's line, a thorough physical inspection for evidence of a wiretap is made by trained personnel at the customer's premises and at all other locations where his circuitry might be exposed to a wiretap. If no evidence of a wiretap is found, the customer is so informed. Where evidence of a wiretap is found, the practice generally is to report to law enforcement authorities any device found in the course of the Company inspection, for the purposes of determining whether the device was lawful and of affording law enforcement an opportunity to investigate if the tap was unlawful. The existence of the device is also reported to the customer requesting the check, generally irrespective of whether it was lawful or unlawful. The customer is told that "a device" has been found on his line, without our characterizing it as lawful or unlawful. Should the customer have any questions, he is referred without further comment to law enforcement.

New Jersey Bell, however, as a matter of policy, informs a customer requesting a wiretap check that only the presence of an unauthorized device will be disclosed. Minnesota by statute similarly limits disclosure to unlawful devices. Should the customer inquire about the presence of a lawful device, he will usually be assured that applicable Federal and State laws require any judge authorizing or approving a court-ordered interception to notify the affected customer within 90 days after interception ceases (or at a later date, if disclosure is postponed upon a good cause showing by law enforcement).

All Bell System Companies report the existence of an unlawful device to the customer requesting the check, as well as to law enforcement (upon authorization from the customer, in the instance of one Company), and the latter is provided an opportunity to investigate for a reasonable period, generally 24-48 hours, prior to removal of the wiretap.

We might point out that unless the wiretap effort is amateurish, a person whose line is being tapped will not hear anything unusual, because of the sophisticated devices employed. As we previously said, most of the complaints originate because the customer hears an odd noise, static, clicking, or other unusual manifestations. As far as our experience discloses, these usually turn out to be difficulties in transmission or other plant irregularities. From 1967 onward, for example, the total number of wiretap and eavesdrop devices of all types (including both lawful and unlawful) found by telephone employees on Bell System lines has averaged less than 21 per month—an average of less than one a month for each of the twenty-four operating companies of the Bell System. In our opinion, the criminal sanctions imposed by Title III (for the unauthorized interception or disclosure or use of wire or oral communications, or the manufacture, distribution, possession, or advertising or intercepting devices), coupled with vigorous law enforcement and attendant publicity, appear to have contributed significantly to safeguarding telephone privacy.

II

In the area of court-ordered wiretapping, it is the policy of the Bell System to cooperate with duly authorized law enforcement authorities in their execution of lawful interceptions by providing limited assistance as necessary for law enforcement to effectuate the particular wiretap. We wish to stress that the Bell System does not do the wiretapping. The assistance furnished generally takes the form of providing line access information, upon the presentation of a court order valid on its face, as to the cable and pair designations and multiple appearances of the terminals of the specific telephone lines approved for interception in the court order.

The term "cable and pair" denotes the pair of wires serving the telephone line in question, and the cable (carried on poles, or in conduit, or buried in the earth) in which the pair reposes. A "terminal" is the distribution point to which a number of individual pairs of wires from the cable are connected, to provide service in that immediate area. A terminal may in a residential area be on aerial cable suspended from telephone poles or on a low, above-ground pedestal, or be found in terminal boxes or connecting strips in the basement, hall, or room of an office building or apartment house. The pair of wires of each telephone serviced from a particular terminal are interconnected at that terminal with a specific pair of wires from the cable, so that a continuous path of communication is established between the customer's premises and the telephone company's central office. The terminals vary in size, depending upon the needs of the particular location. To provide optimum flexibility in usage of telephone equipment, the same pair of wires may appear in parallel in a number of terminals, so that the pair can be used to service a nearby location if its use is not required at a particular point. Thus, the term "multiple appearance" denotes the locations where the same pair of wires appears in more than one terminal on the electrical path between the central office and the customer's premises.

In the instance of law enforcement authorities of the Federal government (and of those States enacting specific enabling legislation in conformity with the amendments to §2518(4) of Title III of the Federal Omnibus Crime Control Act effective February 1, 1971), the court order may "direct" the telephone company to provide limited assistance in the form of the "information, facilities, and technical assistance" necessary to accomplish the wiretap unobtrusively and with a minimum disruption of service. Upon the receipt of such a directive in a court order valid on its face, our cooperation will usually take the form of furnishing a private line channel from terminal to terminal (*i.e.*, a channel from a terminal which also services the telephone line under investigation to a terminal servicing the listening post location designated by law enforcement). Additionally, the above-described line access information will be furnished for the specific telephone lines judicially approved for interception.

On occasion, assistance in the form of private line channels is furnished to Federal authorities in national security cases. This assistance is only rendered upon specific written request of the Attorney General of the United States or of the Director of the Federal Bureau of Investigation (upon the specific written authorization of the Attorney General to make such request) to the local telephone company for such facilities, as a necessary investigative technique under the Presidential power to protect the national security against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. For reasons of security, we are not informed in such cases of the specific nature of the national security matter under investigation.

In cooperating in court-ordered and national security cases, we endeavor to provide the very minimum assistance necessary to effectuate the particular wiretap. Under no circumstances, do we do the wiretapping itself; that is the exclusive province of the appropriate law enforcement officers. Nor do we furnish them with end equipment to be used in connection with a wiretap, such as pen registers, Touch-Tone dial impulse decoders, or tape recorders. Nor do we design or build wiretap or eavesdrop devices for law enforcement authorities. Furthermore, our telephone companies do not train law enforcement personnel in the general methods of wiretapping and eavesdropping, nor do we provide telephone company employee identification cards, uniforms or tools, or telephone company trucks.

As we have repeatedly stated to the Congress, the Federal Communications Commission, and our customers, it has been longstanding Bell System policy to ensure against the unauthorized disclosure of information relating to the existence or contents of any telephone conversation. Accordingly, we have always held toll billing information pertaining to our customers in strict confidence, divulging it only pursuant to lawful process, upon proper demand. We believe this reflects the intent of Congress and the thrust of the law, as well as sound policy.

By way of background, toll billing records are corporate records maintained by each telephone company in the ordinary course of business as necessary substantiation for its charges billed to subscribers. These records consist primarily of toll billing statements, and traffic operator tickets and automatic billing data used in the preparation of such statements. The records are generally kept for a fixed period of time, to serve the needs of the business and conform to statutory and regulatory requirements. They are normally destroyed as a matter of business routine at the conclusion of the retention period, usually six months.

These records are maintained for all subscribers, and not just for those under governmental investigation. They contain no information concerning the contents of any telephone conversation or, with the limited exception of certain collect and person-to-person calls, the identities of the actual parties participating therein.

Prior to March 1974, it was the policy and practice of all Bell System Companies to disclose toll billing information upon receipt of a subpoena duces tecum (such as that of a court of competent jurisdiction, a grand jury or a Congressional committee) or an administrative summons (from the Internal Revenue Service, for example) valid on its face. Additionally, about half of our Companies released such records upon "demand of other lawful authority" such as a letter of demand, generally on official stationery, signed by the principal prosecuting attorney of a state or principal political subdivision thereof or by a law enforcement officer of command rank (usually captain or higher), stating that specific existing toll information for a specified period of time was required in conjunction with an ongoing criminal investigation.

When, however, official copies of subscriber toll billing records were to be introduced in any legal proceeding, such as at a trial or before a grand jury, it was the practice of all Bell System Companies, as a matter of policy, to release such original records only upon receipt of a valid subpoena or administrative summons.

The Federal Communications Commission's Common Carrier Bureau had in 1973 carefully reviewed the restrictions voluntarily imposed by the Bell System upon disclosure of its toll billing records and found them more stringent than was required under Section 605 of the Communications Act and judicial decisions thereunder.

The confidentiality of our customers' communications was further strengthened when, in the course of our continuing review of these matters, the procedures were revised effective March 1, 1974 to provide that no Bell System Company will release customer toll billing records except under valid subpoena or administrative summons. Thus, as a matter of policy, these records are no longer disclosed pursuant to other lawful demand.

In addition, customers are to be automatically notified whenever toll billing records relating to them have been subpoenaed or summoned, except in those circumstances where a legislative committee or law enforcement agency seeking such records requests nondisclosure by certifying that notification could impede and obstruct its official investigation or interfere with enforcement of the criminal law.

Automatic notification to the customer is two-fold: a telephone call the same day that the subpoena or summons is received, followed by written notification within 24 hours. The notification contains all pertinent information, including the name of the party subpoenaing the records and the approximate date upon which they will be furnished.

An exception to the foregoing policies is made in the instance of national security. In such cases, the records are provided only upon specific written request of the Director of the Federal Bureau of Investigation, or of an Associate Director or Assistant Director, for such information, as a necessary investigative technique under the Presidential power to protect the national security against actual or potential attack or hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Notification is not provided to the customer.

Bell System policy regarding the disclosure of its toll billing records strikes, we believe, a proper balance under existing law. It reflects our traditional concern for and society's growing insistence upon preserving the privacy of communications. It recognizes too our obligations to comply with the mandates of lawful process and not to unduly impede official investigations, whether criminal or legislative in character. In these matters we are, in a very real sense, caught in the middle of controversy. The extent to which privacy of communications in this area should yield and where the line between individual privacy and police powers should be drawn in the public interest are, in our opinion, matters of national public policy, to be determined by the Congress after careful evaluation of the countervailing interests.

IV

Turning now to another area of the Commission's inquiries—the measures we employ to combat the theft of telephone service by those clandestinely using electronic toll fraud devices—the Bell System firmly believes that whenever a communication is lawfully placed, its existence and contents must be afforded the full protection of the law.

But when wrongdoers break into the telephone network and by use of an electronic device seize its circuits so that calls can be illegally initiated, we are faced with the formidable problem of gathering evidence of such fraud for purposes of prosecution and billing. Telephone service is our only product, and its wholesale theft results in losses ultimately borne by the honest telephone user.

The Communications Act of 1934 imposes upon us the statutory obligation to prevent such thefts of service. In essence, the Act imposes upon each telephone company the duty to require all users of its service to pay the lawful charges authorized by tariffs on file with the appropriate regulatory bodies. No carrier may discriminate between its customers by granting preferential treatment to any. Knowingly to allow those committing electronic toll fraud to receive "free service" would constitute such discrimination.

Furthermore, each telephone company is enjoined, under pain of criminal penalty, from neglecting or failing to maintain correct and complete records and accounts of the movements of all traffic over its facilities. Each carrier is also obliged to bill the federal excise tax on each long distance call.

To put the matter of electronic toll fraud into historical perspective—in the early Sixties, a most ominous threat burst upon the scene, the advent of the so-called black and blue boxes. These devices enabled the user to circumvent the telephone company's automatic billing equipment and thereby illegally receive or place calls without payment of the lawful charges. A "black box" is operated by the called party, so that anyone calling that number from any location is not charged for the call. Contrariwise, a "blue box" is operated by the calling party and,

because of its small size and portability, can be hidden on the person and at any time used to place an illegal call from any telephone to anywhere in the world (often by merely holding the device against the telephone's mouthpiece, without the necessity of wiring it into the line).

It was recognized that if such fraud could be committed with impunity, losses of staggering proportions would ensue. Faced with this threat, the Bell System took immediate steps to determine whether it would be necessary to undertake the monumental task of redesigning and restructuring the signalling functions of the nationwide telecommunications network—at an estimated cost to our customers ranging upward to one billion dollars. Bell Laboratories was asked to develop electronic toll fraud detection equipment to enable the Bell System to ascertain the magnitude of the fraudulent calling.

From the inception of the project, the following guidelines were established to ensure, among others, that privacy of communications would be fully safeguarded:

- The initial scanning and testing would be confined to randomly sampling a limited number of trunk lines handling outgoing long distance calls at a few representative cities.

- The scanning and testing would be automatically accomplished by mechanical means, without the intervention of the human ear.

- Recording for subsequent analysis would be confined to those calls, which when initially scanned and tested, exhibited to the equipment preliminary indications of illegality (e.g., abnormal network tones and signalling).

- These recordings were to be immediately sealed and dispatched to a centralized toll fraud Analysis Bureau to be established by AT&T in New York City.

- The voice recording for analysis phase would cease when other technological methods of detecting preliminary indications of illegal calling on the network were developed.

Beginning in late 1964, six "first generation" toll trunk test units, developed by Bell Laboratories principally from standard telephone components, were placed in service at the following locations: two in New York City, two in Los Angeles, and one each in Miami and Detroit. To obtain more effective sampling, one of the New York units was moved to Newark in late 1966, and the Detroit unit was relocated to St. Louis in early 1967.

These units were fully automatic and housed in locked cabinets located in secure areas in telephone company long distance switching centers. Each unit could scan only five calls at any one time, randomly selected from the traffic streaming through the one hundred outgoing long distance trunk lines to which the unit was connected. Only when the unit's logic found positive preliminary indications of illegality was any portion of the conversation recorded for subsequent analysis.

It bears reiteration that all scanning, testing and recording by these first generation units were automatically accomplished by mechanical means, without any human participation.

The recordings were placed in sealed containers and dispatched immediately by hand or through registered mail to the Analysis Bureau in New York. The Bureau was manned by a small group of closely supervised, long term management personnel who had been carefully selected and trained for this project. Each call was analyzed for pertinent statistical data and at times also provided leads as to specific offenders. These leads, including until December 1966 extracted informative recordings of suspected blue box calls, were forwarded to the appropriate operating telephone company for investigation. The recordings received by the Bureau were erased within 30 days after analysis.

During the first years of the project, these toll trunk test units were able to gather significant statistical evidence of the widespread nature of the illegal calling. Preliminary information furnished by these units ultimately produced a number of successful prosecutions of major offenders, many of whom were associated with organized crime.

The project was terminated in May 1970. By that time, Bell Laboratories had developed to the field trial stage more sophisticated "second generation" equipment which permitted more effective scanning and testing of the telecommunications network for preliminary indications of electronic toll fraud, without the necessity of voice recording during the pre-investigative detection stage. Extensive use was also being made of computers, plant testing equipment and procedures, and statistical analyses. Nonetheless, despite these and other efforts and our constant vigilance, electronic toll fraud continues at flood level.

Because blue and black box devices are relatively inexpensive to make, their use has grown at an alarming rate. We estimate blue boxes can be mass-produced at a cost of \$25 to \$50 per unit, and black boxes at a cost of a dollar or less. Our experience has shown that these devices have a unique appeal to, among others, the criminal element, whether it be a member of organized crime or an unprincipled businessman. This is so because not only is payment of the lawful telephone charges evaded, but also any record of the communication concealed, permitting them to conduct their unlawful activities under a smoke screen of anonymity.

Such crimes have never enjoyed the protection of the law, neither before nor after the passage of Title III of the Federal Omnibus Crime Control and Safe Streets Act in June 1968. A substantial number of distinguished courts, including several United States Circuit Courts of Appeals, have unequivocally held that persons stealing telephone service by trespassing upon the telephone network place themselves outside the protection of Section 605 of the Communications Act, and of Title III. In these criminal cases, our entire process of gathering evidence has been subjected to close and thorough judicial scrutiny. This judicial oversight has continued to date, with some 325 convictions and a number of pending cases, indicating the extent to which the courts at federal and state level have repeatedly reviewed telephone company procedures for gathering such evidence. With virtual unanimity, the courts have held that the methods used have been lawful, independent of cooperation with law enforcement authorities, and wholly in the public interest.

It should be stressed, too, that prosecution has been and continues to be the only effective deterrent. As to the specific methods employed by the telephone companies to gather evidence of electronic toll fraud—in contradistinction to the previously described pre-investigative preliminary scanning of the network—we have found that a minimum amount of recording of a limited number of calls is indispensable, if a prosecution is to succeed.

Since the goods being stolen are the communication itself (for example, by a blue box user), there is no alternative at this state of the art but to make, for prosecutory purposes, a limited recording of each illegal call, at least of the fraudulent dialing, ringing, and opening salutations, to:

- identify the calling party (the user of the blue box), and others with whom he may be acting in concert;

- Identification of the telephone line(s) from which the fraudulent calls are originating must be followed by the more difficult identification of the specific individual(s) making the calls. This is of paramount importance.

- establish, corroboratively, the location(s) from which the specific calls upon which prosecution is to be based are originating;

- record with respect to each such call the multifrequency tones being "dialed" (key pulsed) by the blue box; and

- determine whether the fraudulent call (or series of calls) was completed by the called party (parties) answering.

Distance (as well as time) is a factor in determining the proper billing charge for a long distance call. It is, therefore, necessary to ascertain each specific location called after the wrongdoer seizes the circuit. Let us assume, for example, that a blue box user

places a call from Washington, D.C. to the directory assistance operator at Chicago (312 555-1212). By then emitting a specific tone from his blue box device, the user can disconnect the operator and seize the long distance circuit "at Chicago." He can then dial from that point to any part of the country or to London, Moscow, Sydney, and other parts of the world.

The ultimate destination of each blue box call can, therefore, be determined only by documenting the multifrequency tones key pulsed. Also, as previously explained, after seizing the circuit the blue box user can make a series of calls. Should such fraudulent calls be key pulsed, determination of whether each such call was completed can only be made through recording the telltale tones. Unless the tones are captured at the very moment they are emitted, they are of course "lost forever."

Complete documentation of the requisite evidence cannot be obtained by use of regular plant testing equipment such as a peg count register (a simple electromechanical counting device that will count blue box tones). Such equipment cannot identify the fraudulent caller, nor determine whether each such call was completed, nor produce other necessary evidence. These essential evidentiary elements can only be adduced through recording.

Nor will inspection of the suspect location usually uncover the small, readily-concealed devices. Moreover, seizure of the device would not, in and of itself, establish that fraud by wire had been committed, nor by whom, nor the extent of the fraud. Nor can the Automatic Message Accounting equipment that normally obtains the information essential for billing purposes produce the necessary evidence of toll fraud.

Most importantly, the limited recording done is solely to gather evidence of calls illegally placed. This is not a "wiretapping case," where the contents of the conversations are sought as evidence of some crime other than the theft of service itself.

Limited recording by the local telephone company is done from secure locations, admission to which is tightly controlled on a "need to know" basis. This is done to maximize the protection of customers' privacy by preventing intrusion by unauthorized personnel. These quarters are kept under lock and key when not in use.

To assure the privacy of lawful communications, the telephone companies first employ a series of investigatory measures other than voice recording (e.g., a peg count register or its equivalent) to carefully evaluate the accuracy of any preliminary indications of electronic toll fraud. Only when a reasonable suspicion of such fraud has been firmly established, the possibility of plant trouble ruled out, and all other investigative measures exhausted, do the telephone companies engage in limited recording.

Recording does not begin until the caller's blue box emits a tone to seize the line. The recording is brief and usually includes:

- (i) the dialing of the multifrequency tones of the number being illicitly called;

- (ii) the ensuing ringing cycle; and

- (iii) the opening salutations of the parties after the call is answered. Usually only 60 seconds or less of conversation is recorded. The equipment generally is adjusted to cut off automatically at the end of this recording cycle.

As part of our continuing review of all operating policies relating to the privacy of our customers' communications, we recently further refined our procedures to require that no such limited voice recording may take place without the prior express approval of the Company's Security Manager—and the concurrence of the Vice President—Operations and the Vice President and General Counsel, or their designates. In this respect too our Systemwide procedures are more restrictive than the requirements of the law.

Due to the nationwide character of such fraud, we are of the opinion that a Federal statute proscribing the manufacture, possession, importation, distribution, or advertising of electronic toll fraud devices will substantially contribute to the containment of this threat. Such a statute should also proscribe the publication of plans, specifications and instructions for making, assembling or using these devices. Numerous "how-to-do-it" electronic toll fraud articles, published by national magazines and other periodicals in recent years, graphically illustrate the invidious nature and widespread dissemination of this type of publication.

We have, therefore, submitted to the Commission a proposed statute proscribing these activities. By outlawing such conduct in interstate and foreign commerce, the availability of this narrowly-defined category of electronic toll fraud devices, for which there is no legitimate use, will be substantially curtailed. The statute will also significantly diminish the enticement of others to such criminal activities.

The proposed legislation effectively supplements the Federal "fraud by wire" provisions set forth in §1343 of 18 U.S.C., which prohibits the use of toll fraud devices in interstate or foreign commerce. However, prosecution under the "fraud by wire" statute, which criminalizes the use of the device, will necessarily continue to be our first line of defense and principal deterrent. Also, as previously noted, at the present state of the art a minimal amount of recording of a limited number of calls will remain indispensable to the success of any such prosecution.

In summary, we have shown that at best, detection of electronic toll fraud is difficult. We can only conjecture at the full scale of the substantial revenue losses sustained by the telephone industry and its customers. As in many criminal areas where detection is difficult, the instances of electronic toll fraud unearthed by the telephone companies represent merely that

portion of the iceberg visible to the eye. The actual losses currently being sustained may be ten or twenty times as great as our provable losses.

In none of the cases prosecuted, state or federal, has any judge ever subscribed to the thesis that the telephone companies do not have the statutory obligation to collect, through limited recording, the evidence necessary to identify those placing calls in an illegal manner. To hold otherwise would, in effect, herald to the racketeer, the corrupt businessman, and all others that they have carte blanche to operate with relative impunity.

The virtually unchecked use of electronic toll fraud devices which would ensue if the threat of detection and prosecution is removed would impose an overwhelming financial burden on the telephone industry and its honest customers, who would be required to underwrite the entire cost of these depredations, including the total loss of revenue and the substantial expense of the circuits, facilities, and equipment tied up by such illegal use. These losses would rapidly reach staggering proportions, soaring into the tens and hundreds of millions of dollars and jeopardizing our very ability to provide telephone service to this nation.

V

The foregoing reflects our experience in the areas of wire-tapping and electronic surveillance, the disclosure of toll billing information, and electronic toll fraud prior and subsequent to the passage of Title III of the Federal Omnibus Crime Control Act in 1968, and our continuing efforts to maximize the privacy accorded to communications.

We wish to assure you that the Bell System continues to be wholly dedicated to the proposition that the public is entitled to telephone communications free from unlawful interception or divulgence. We are vitally interested in the protection of the privacy of communications and always welcome measures and techniques that will strengthen and preserve it.

I shall be pleased to answer any questions the Commission may have.



AT&T

American Telephone and
Telegraph Company
195 Broadway
New York, N. Y. 10007
Phone (212) 393-9800

August 22, 1975

Mr. Kenneth J. Hodson
Executive Director
National Commission for the
Review of Federal and State
Laws Relating to Wiretapping
and Electronic Surveillance
1875 Connecticut Avenue, N.W.
Washington, D.C. 20009

Dear Mr. Hodson:

This is in response to inquiries made by members of the Commission and its staff during the course of my testimony before the Commission on June 27, 1975.

I

In my letter to you of January 13, 1975, we enclosed a 20-page report, entitled "Bell System - Illegal Wiretaps Found January 1, 1967 to June 30, 1974," which disclosed the number of illegal wiretapping and eavesdropping devices found in the United States by Telephone Company personnel on the lines (facilities, equipment, and instruments) of the Associated Operating Companies of the Bell System.

In such letter, we also informed the Commission that it was the general practice of all Bell System Companies, with one exception (Illinois Bell Telephone Company), to notify the affected customer and the appropriate law enforcement authorities, whenever such a device is found on a customer's line. We said that in the instance of Illinois Bell, it had been the longstanding practice to notify only the customer upon whose line the device was found and, further, to assure the customer that should he or she wish to report the incident to law enforcement, the Company would fully cooperate with such authorities in any ensuing investigation of the matter.

We also alluded to this subject in my written Statement to the Commission of June 27, 1975, saying on Page 7 thereof that all Bell System Companies report the presence of an unlawful device to the customer requesting the check, as well as to law enforcement (upon authorization of the customer, in the instance of one Company - Illinois Bell), and the latter is provided an opportunity to investigate for a reasonable period, generally 24-48 hours, prior to removal

of the wiretap. During my testimony, there was a brief colloquy on the practice of Illinois Bell. [Tr. 148-50]*

We wish to advise the Commission that Illinois Bell has revised its reporting procedures to conform to Bell System recommended practice. Accordingly, it is now the general practice of all Associated Operating Companies of the Bell System, including Illinois Bell, to notify both the affected customer, and the appropriate law enforcement authorities, whenever an illegal wiretapping or eavesdropping device is found on a customer's line.

II

During the hearing, question was raised as to whether Bell System Companies maintain a record of the number of occasions annually on which it was necessary to conduct a physical inspection of the customer's premises in the course of handling a customer's request that his or her line be checked for a possible wiretap. [Tr. 145-46] Despite the extensive recordkeeping regularly maintained in this area by our Companies, evidenced in part by the detail contained in the aforementioned 20-page report on illegal wiretaps found furnished to the Commission under date of January 13, 1975, it has not been the general practice of the Associated Operating Companies of the Bell System to maintain a specific record of the requested information regarding physical inspections on customer premises.

In this connection, it appears appropriate to reiterate our testimony of June 27, 1975 that most of the wiretap complaints lodged by customers originate because the customer hears an odd noise, static, clicking, cross talk, or other apparently unusual manifestations. Insofar as our experience discloses, these usually turn out to be difficulties in transmission or other plant irregularities which can be promptly detected. In the small number of cases where no trouble is detected in testing a customer's line, a thorough inspection for evidence of a wiretap is made by trained Telephone Company personnel at the customer's premises and at all other locations where his or her circuitry might be exposed to a wiretap.

You may recall that on June 19, 1975 we furnished the Commission with the following updated tabulation of the

* All Transcript citations herein in brackets refer to pagination of the unedited version of the Transcript of the Commission's hearing of June 27, 1975.

"Total Number of Wiretapping and Eavesdropping Devices Found in the United States by Telephone Company Personnel on the Lines (Facilities, Equipment and Instruments) of the Associated Companies of the Bell System" during the calendar years 1967 - 1974:

<u>Year</u>	<u>Total</u>	<u>Year</u>	<u>Total</u>
1967	195	1971	249
1968	179	1972	174
1969	218	1973	163
1970	195	1974	182

Thus, from 1967 onward the total number of wiretap and eavesdrop devices of all types (including both lawful and unlawful) found by Telephone Company employees on Bell System lines has averaged less than 21 per month - an average of less than one per month for each of the twenty-four Associated Operating Companies of the Bell System.

Further, these total annual figures include all of such devices found, whether as a result of one of the 10,000 or so customer requests for a wiretap check made Bell Systemwide each year or through detection by Telephone Company personnel in the regular course of their work (e.g., by one of the 90,000 employees whose daily work assignments are in outside plant). [Tr. 144-45]

Thus even if we, conservatively, eliminate from consideration those of the above-listed devices which were found by Telephone Company employees in the normal performance of their duties (rather than as a consequence of a customer request for a wiretap check), it has been our Bell Systemwide experience that in only some 2 percent of the 10,000 or so customer requests received per year has a device actually been found.

III

In accordance with the Commission's request [Tr. 131], enclosed are photographs of the two electronic toll fraud devices which were displayed and the operation of each described during my testimony of June 27, 1975, Exhibit "A" being a photograph of the "black box" and Exhibit "B" of the "blue box."

It will be recalled that these electronic toll fraud devices enable the user to circumvent a telephone company's automatic billing equipment and thereby illegally receive or place calls without payment of the lawful charges. A "black box" is operated by the called party, so that anyone calling that number from any location is not charged for the call. Contrariwise, a "blue box" is operated by the calling party and, because of its small size and portability, can be concealed on the person and at any time used to place an illegal call from any telephone to virtually anywhere in the world (often by merely holding the device against the telephone's mouthpiece, without the necessity of wiring it into the line).

IV

In December 1966, the longstanding Bell System prohibition against accepting in the Yellow Pages of its telephone directories advertisements by private detective agencies and others, stating or implying that the services being offered included the use of wiretapping, was expanded to prohibit too the acceptance of eavesdropping copy. This standard, adopted by all Bell System Companies, was interpreted from the outset to make equally unacceptable so-called debugging advertising (i.e., advertising stating or implying electronic devices or services will be provided for the detection and removal of wiretaps and eavesdropping "bugs"), on the theory that those who can debug also possess the capability to bug and wiretap.

Enclosed for the information of the Commission in accordance with its request [Tr. 151-52], as Exhibit "C", is a decision of the Missouri Public Service Commission in the form of a Report and Order in Markowitz d/b/a Monitor Agency v. Southwestern Bell Telephone Company, dated December 7, 1971, upholding as nondiscriminatory, and by implication in the public interest (see, for example, the Commission's statement on Page 2 thereof that there had been no complaint "as to the reasonableness of the standard in question"), Southwestern Bell's refusal to accept debugging advertising copy from a private detective agency for inclusion in the Yellow Pages of its telephone directories.

Also enclosed as Exhibit "D" is a decision of the United States District Court for the Eastern District of Missouri, Eastern Division (St. Louis) in the form of a Memorandum, Order and Judgment in Markowitz v. AT&T and Southwestern Bell Telephone Company, dated June 22, 1973,

granting defendants' motions for summary judgment in an ensuing action by the same plaintiff for monetary damages. The Court concluded that the doctrine of collateral estoppel precluded relitigation of facts determined adversely to the plaintiff in the above-mentioned prior proceeding before the Missouri Public Service Commission.

V

During the hearing, inquiry was made concerning the provision by a local telephone company of a connection (in the nature of an off-premises extension) of a customer's line to a telephone answering bureau, to enable the latter to answer calls and perform such other secretarial-type services as the customer may require. [Tr. 192-96]

As a measure for the protection of privacy of communications, it is Bell System policy to verify in writing any customer order and concomitant authorization to provide such service, whether the request is made by the customer, orally or in writing, directly to the local telephone company or through a telephone answering bureau. Written verification is accomplished by the appropriate business office of the local telephone company promptly sending a letter of confirmation to the customer at the address in question, confirming the customer's order to connect the secretarial-type telephone answering service, stating the charges therefor, and furnishing other information relevant to the provision of the service.

Each Bell System Company promptly and thoroughly investigates any complaint alleging improper use of telephone answering service, whether the complaint is presented directly to it or received through regulatory or other channels. Whenever the circumstances so warrant, necessary corrective action is taken by the Telephone Company to ensure that the telephone answering bureau's practices are brought into strict compliance with applicable tariff and other legal requirements. Should the investigation disclose that the secrecy of a customer's communications has been unlawfully breached, the matter is also immediately referred to the appropriate law enforcement authorities.

Over the years, however, Bell System Companies have received extremely few complaints or other indications of abuse of this particular service. This favorable experience appears to reflect, in large part, the responsible approach

of the businesses providing telephone answering service, the owners of which are often people of modest means who depend upon the success of their respective local enterprises for their livelihood. Many of the operations are small in scale and performed with few employees. There is full recognition of the vital importance of an unblemished reputation to the success of the enterprise, and that any act of misconduct by unlawful or improper invasion of a client's privacy of communications would seriously damage, if not destroy, their business, as well as invoke criminal sanctions.

VI

As stated at the hearing during the colloquy on the applicability of Title III of the Federal Omnibus Crime Control Act to data communications [Tr. 189-92], we are of the opinion that the Act's proscriptions against the unauthorized interception, use or disclosure of the contents of a wire communication are intended to encompass all forms of information transmitted, in whole or in part, over the facilities of a communications common carrier, whether by way of a two-way voice conversation, a data transmission, or other form of communication (e.g., telephotograph and teletypewriter transmissions).

This conclusion regarding the intendment of Congress in enacting such sweeping legislation designed "to protect effectively the privacy of wire . . . communications" [§ 801(b), Title III] finds support in the following comment of the Senate Judiciary Committee in its landmark Senate Report No. 1097 of April 29, 1968, on Page 89 thereof [2 U.S. Cong. & Adm. News 1968 at 2178]:

"Paragraph (1) defines 'wire communication' to include all communications carried by a common carrier, in whole or in part, through our Nation's communications network. The coverage is intended to be comprehensive." (Emphasis supplied.)

It is to be borne in mind that all information transmitted over the telephone network is in the form of electrical signals. This is true, irrespective of whether the communication originates as a voice signal, encoded data information, or other form of communication. Thus, when an electronic, mechanical or other device intercepts the contents of any wire communication, within the meaning ascribed to each of these terms by Title III (§ 2510 of 18 U.S.C.), there is

in each instance only an "aural acquisition" of electrical signals - regardless of the type of communication transmitted. Accordingly, the interceptions of a data communication would appear to be as unlawful as the interception of a wire conversation.

Should the Commission conclude, however, that it would be advisable to clarify the existing statutory language, so as to remove any doubt and ensure the applicability of the proscriptions of Title III to the transmission** of all forms of communication, we would suggest that the Act be amended in the following two respects:

(i) Revise the definition of "wire communication" in § 2510(1) of 18 U.S.C. to read as follows:

"(1) 'wire communication' means any communication made in whole or in part through the use of facilities for the transmission of ~~[communications]~~ writing, signs, signals, data, pictures, and sounds of all kinds by the aid of wire, cable, or other like connection between the point of origin and the point of reception furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications;"
(Underscoring denotes newly added language; brackets denote deleted language.)

As so amended, the definition expressly covers the transmission of all forms of communication. It closely corresponds to the definition of "wire communication" contained in Section 3(a) of the Communications Act of 1934, as amended. (47 U.S.C. § 153(a))

(ii) Revise the definition of "intercept" in § 2510(4) of 18 U.S.C. by deleting the word "aural" from the term "aural acquisition":

"(4) 'intercept' means the ~~[aural]~~ acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device." (Brackets denote deleted language.)

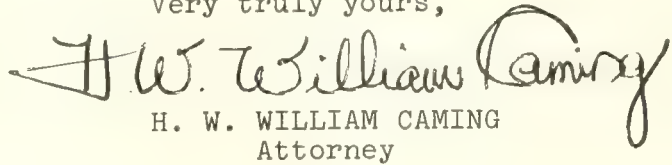
** Inasmuch as the Act is confined to the transmission of wire communications, the proposed amendatory language does not purport to reach acts of misconduct such as the unauthorized, tortious inclusion, modification, or deletion of encoded data information stored in computers.

Mr. Kenneth J. Hodson

* * * * *

We trust the foregoing provides the Commission
with the desired information.

Very truly yours,


H. W. WILLIAM CAMING
Attorney

Enclosures

BEFORE THE PUBLIC SERVICE COMMISSION
OF THE STATE OF MISSOURI

In the matter of the complaint of M. M. Markowitz, d/b/a
Monitor Agency, 1231 Kurt Street, St. Louis, Missouri,
Complainant,

vs.

Southwestern Bell Telephone Company, St. Louis, Missouri,
Respondent.

APPEARANCES:

Darwin Portman and Edwin Harrison,
Attorneys at Law, 611 Olive, St. Louis,
Missouri, for Monitor Agency.

James R. Taylor and John D. Rahoy,
Attorneys at Law, 100 North 12th, Room 630,
St. Louis, Missouri, for Southwestern Bell
Telephone Company.

Richard T. Ciottonne, Assistant General Counsel, Public Service
Commission, Jefferson State Office Building, Jefferson City,
Missouri, for the Staff and the Public.

REPORT AND ORDER

On January 19, 1971, the Commission received a complaint in the above-styled case, regarding telephone directory listings of the Complainant, M. M. Markowitz, doing business as Monitor Agency, 1231 Kurt Street, St. Louis, Missouri. On the 27th day of January, 1971, the Commission issued its Order To Satisfy Or Answer.

On the 8th day of February, 1971, Southwestern Bell Telephone Company (Respondent) filed its Answer To Complaint. On February 26, 1971, the Commission issued its Order and Notice Of Hearing in the above-styled case. On March 4, 1971, the Respondent filed its Motion For Continuance, which was granted by Order of this Commission on March 9, 1971, and the case was set for hearing on April 14, 1971. A hearing was held on April 14, 1971 and continued to May 21, 1971 and the hearing was concluded on that date.

At the conclusion of the hearing, Applicant and Respondent requested the filing of briefs but did not request oral argument before the entire Commission and waived the reading of the transcript.

Simultaneous briefs were ordered to be filed three weeks after the filing of transcript and reply briefs if any ten days after the filing of simultaneous briefs.

The Respondent, Southwestern Bell Telephone Company, filed its brief on July 14, 1971. The Complainant filed his brief on September 23, 1971, and the Respondent filed its reply brief on October 12, 1971. The Complainant did not file a reply brief.

On November 30, 1971, the Complainant filed a "Petition To Set Aside Submission And Reopen Proceedings For The Taking Of Additional Evidence And Modification Of Complaint."

Findings of Fact

The Missouri Public Service Commission, having considered all of the competent and substantial evidence upon the whole record, makes the following findings of fact:

Marty Markowitz, doing business as Monitor Agency, (Complainant), 1231 Kurt Street, St. Louis, Missouri, complains of "two types of discrimination practiced against him by Respondent, Southwestern Bell Telephone Company in its Yellow Pages Directories:

1. Discrimination against him, and in favor of certain of his competitors, in the 1967 and 1969 St. Louis Yellow Pages Directories
2. Discrimination within the class of detectives on a geographic basis within the State of Missouri. And, Complainant

further complains of the arbitrary and capricious interpretation and application of the "standards" promulgated by Respondent from time to time which 'allegedly' resulted in the above instances of discrimination against him." The Complainant does not complain as to the reasonableness of the standard in question. The standard in the instant case involved the application to the Complainant of Southwestern Bell Yellow Page Standard No. 25. This Standard appears in Respondent "Yellow Pages Specifications And Standards" booklet attached to Respondent's Answer in this case. The specifications portion of this booklet applies to all paid advertising, and generally governs the size and layout of particular advertisements. The standards portion of the booklet governs the permissible content of paid advertising. Many of the standards if general in nature apply to all paid advertising. Some of the standards are more particular in nature and apply to only certain classifications that appear within the yellow pages directories. These standards are promulgated and in force by the Respondent in an effort to protect its customers, its advertisers, and the general public from misleading, immoral, illegal, undesirable and harmful advertising. According to the Respondent they are also promulgated and enforced in an effort to maintain the integrity of Southwestern Bell and of the directories it publishes. The Respondent's directories standards are at times based upon investigation and recommendations of a directory ethics committee sponsored by the American Telephone and Telegraph Company. This committee is composed of various representatives from Bell companies and also from independent telephone companies. The findings and conclusions of this committee concerning the need for adoption of new yellow page standards are sent to directory representatives in various Bell companies, and usually to the directory headquarters. These findings and conclusions are no more than recommendations and are not binding upon the individual companies. Each company has the right to make its own decision as to the adoption in whole or in part of any recommended standard. The Respondent first filed its Yellow Pages Specifications And Standards with this Commission in 1962. The Respondent filed its current standards with the Commission attached to its Answer to the Commission's Order to Satisfy or Answer on February 8, 1971.

The Respondent's Yellow Page Standard No. 25 and referred to by the Respondent's witnesses as "the invasion of privacy" standard reads as follows:

Advertising copies stating or implying that wire tapping is employed should not be accepted. Equally unacceptable is the offering of electronic devices or of services involving the use of such devices which may cause the invasion of privacy by eavesdropping

This standard was first made applicable in the St. Louis area for the 1967 Yellow Page issue. It was determined by the Respondent that for the 1967 St. Louis Yellow Pages detective agencies could not use the words "bugging" or "debugging" in their advertising, nor could they advertise the ability to place concealed listening devices, nor could they advertise their ability to detect and remove such listening devices. In 1968, the invasion of privacy standard was modified to prohibit detectives or private investigators from advertising the ability to detect and remove electronic devices. This modification of the invasion of privacy standard was based upon the conclusion reached by the St. Louis area directory personnel that advertising the ability to detect and remove hidden electronic devices was, in fact, also advertising the ability to place those same devices.

The Complainant is licensed as a private investigator in St. Louis County, Missouri. In 1964 he began working in the private investigating business on a part-time basis; and in 1967 became a full-time private investigator. The Complainant holds himself out as an expert in the detection and removal of electronic eavesdropping equipment and devices because of his special equipment and because of his previous training in this field. The Com-

plainant's private investigating business is limited primarily to the St. Louis area. He has not held himself out as competing with detectives in Springfield, Kansas City, or any other place outside of the St. Louis area.

In February of 1967 the Complainant contacted Southwestern Bell Telephone Company in St. Louis with the desire to place an advertisement under the "Detective" classification of the 1967 St. Louis area yellow pages. On the 10th day of February, 1967, Mr. John Meltner, a Southwestern Bell directory salesman, discussed the proposed advertisement with Complainant. The advertisement proposed by Complainant was not acceptable according to Mr. Meltner on the basis that it violated recently implemented invasion of privacy standard (Standard No. 25). According to Complainant, the reason advanced by Mr. Meltner for the refusal of the advertisement was because it contained the word "detection." However, according to Mr. Meltner the proposed advertisement was objectionable because it contained either the word "bugging" or "debugging". The Complainant denied that the proposed advertisement contained the word "bugging", however, Complainant identified Respondent's Exhibit B as a copy of the proposed advertisement, which he had prepared for Mr. Meltner's approval. Respondent's Exhibit B was not a copy of the original proposed advertisement. The original had been either lost or destroyed by Complainant. Exhibit B, however, was prepared by Complainant prior to the time his deposition was taken preparatory to the hearing; it was identified as his best recollection of the draft he had prepared prior to Mr. Meltner's February 1967 visit. Respondent's Exhibit B does contain the word "bugging." Prior to declining the proposed advertisement of Complainant, Mr. Meltner called his directory supervisor, Mr. Schaeffler, and discussed with him the acceptability of the proposed advertisement. Mr. Schaeffler agreed that the proposed advertisement could not be accepted but did suggest certain modifications that would bring it into compliance with the invasion of privacy standard (Standard No. 25). Thereafter, the Complainant and Mr. Meltner conversed and eventually drafted an advertisement which was agreeable to Complainant and would subsequently appear in the 1967 St. Louis Area Yellow Page Directory under the classification "Detectives." The advertisement contained the phrase "removal of electronic devices."

When the 1967 St. Louis Area Yellow Page Directory was issued and the advertisement by the Murco Detective Agency appeared under the "Detective" classification, it contained the word "detection" which the Complainant contends he was prohibited from using. This advertisement is the only advertisement appearing in the 1967 St. Louis Area Yellow Pages that the Complainant complains about. Mr. Meltner and Mr. Schaeffler were both familiar with the content of the Murco advertisement and with the use of the word "detection" at the time of the February 10, 1967 conference with the Complainant and that there was no reason for either of them to deny the use of the word "detection" to the Complainant and they did not do so. If the Complainant had requested the use of the phrase "detection of electronic devices" instead of the phrase "removal of electronic devices" which Complainant did request he would have been allowed to use that phrase for the year 1967 in the St. Louis Area Yellow Pages.

Prior to the closing date of the 1968 St. Louis Area Yellow Pages the Complainant was advised of the modification of the invasion of privacy standard (Standard No. 25). This modification required the Complainant to delete the phrase "removal of electronic devices" which had appeared in his 1967 advertisement, from his 1968 advertisement. After a number of conferences between the Complainant and with various Southwestern Bell directory personnel, the Complainant proposed the use of the phrase "Special Services Unlimited" for the 1967 advertisement under the "Detective" classification. This phrase was drafted by the Complainant and was accepted by Southwestern Bell and

published as advertising for the Monitor Agency for the year 1968. The Complainant does not complain that any advertisement appearing in the 1968 St. Louis Area Yellow Pages under the "Detective" classification was violative of the invasion of privacy standard (Standard No. 25) or was inconsistent with the representations made to him as to the language which was unacceptable in the "Detective" classification.

For the year 1968 the Complainant requested publication of the same advertisement that appeared in the 1967 Yellow Pages for the Monitor Detective Agency.

In the year 1969, the Inter-Tect Detective Agency contracted for its first advertisement to appear in the St. Louis Area Yellow Pages. In the 1969 St. Louis Area Yellow Pages the Inter-Tect advertisement did appear and the advertisement did include the word "debugging" in the text of the advertisement and as admitted by the Respondent, this advertisement was violative of the invasion of privacy standard (Standard No. 25). The Inter-Tect advertisement was requested by that detective agency immediately prior to the closing date of the 1969 directory. The closing date of the directory is that date after which no advertisement will be accepted for publication in that particular directory. The several weeks immediately preceding and following the closing date is the busiest time of the year for directory personnel, compounding the problem of insuring that all advertisements are in compliance with the various applicable directory standards. The directory supervisor in charge of the 1969 Inter-Tect advertisement was critically ill and out of the office at the time that this advertisement was requested. The galley sheet, which is proofread by directory personnel immediately prior to the final printing by the printer in Chicago, Illinois contained a "hole" on the page under the "Detective" classification where the 1969 Inter-Tect advertisement subsequently appeared. A Southwestern Bell employee contacted the printer with reference to this particular advertisement that was to appear in this blank space in the galley sheet. He was informed by the printer that filler copy would be inserted in this "hole". "Filler Copy" is Southwestern Bell advertising copy supplied to the printer to insure proper paging in the directory. Complainant contends that it is not understandable how the inclusion of the objectionable language in the 1969 Inter-Tect advertisement could have been only a good faith error or mistake. However, the St. Louis Area Yellow Pages contain approximately 90,000 paid and non-paid advertisements in its directory. One of the galley sheets for the "Detective" classification of the 1969 St. Louis Yellow Pages submitted to the Respondent's directory personnel by the printer contained what is referred to as a hole or blank space in which the Inter-Tect advertisement was later inserted by the printer. The proofreading of these galley sheets did not result in discovery of the objectionable language as it ordinarily would have. The Respondent's directory personnel assumed that this hole would contain "filler copy". And it was not until the Yellow Pages were published that the Respondent was able to ascertain that an ad violative of its Standard No. 25 was printed. The 1970 Inter-Tect advertisement appearing in the 1970 St. Louis Area Yellow Pages did not contain the objectionable language.

The Complainant did not contract with the Respondent for the placement of any paid advertisement in the 1971 issue of the St. Louis Area Yellow Pages.

The 1968, 1969 and 1970 Springfield and Kansas City Yellow Page directories all contained advertisements in the "Detective" classification which violated the invasion of privacy standard (Standard No. 25). However, the 1971 Springfield and Kansas City Yellow Page directories conformed to Respondent's guidelines. It has taken the Respondent approximately three years to arrive at uniformity in Yellow Page advertising for its "Detective" classification in the Cities of Springfield, Kansas City, and St. Louis, Missouri.

Conclusions

The Missouri Public Service Commission has arrived at the following conclusions:

The Commission does not find from the evidence that the Respondent discriminated unlawfully against the Complainant nor discriminated unlawfully against the class of detectives in regard to those situated in St. Louis and other detectives advertising in the Yellow Pages in Kansas City and Springfield, notwithstanding that detectives in Kansas City and Springfield were allowed to advertise in violation of the invasion of privacy standard for some three years. It is clear from the evidence that the Respondent was making an effort to eliminate such advertising and further that this could not be accomplished at once in all three cities. The 1971 Yellow Page directories all conform to the Respondent's Standard No. 25.

The Commission further concludes that the Inter-Tect advertisement, which appeared in the 1969 St. Louis Area Yellow Pages was the result of a good faith error and was not the result of discrimination against the Complainant.

As the Kansas City Court of Appeals stated in *Videon Corporation v. Burton*, 369 S.W.2d, 264 at 271, in citing *Frank Serpa, Jr. v. Pacific Telephone & Telegraph Co.*, 17 P.U.R.3d, 378 (1957):

Since the publication of advertisements and the listing of businesses in a directory is vital to the proper rendition of telephone service it is a matter within the regulatory jurisdiction of the Commission. However, because the telephone company in publishing the directory is itself a party to any representations therein and to any practices carried on by advertisers therein, it has the duty as well as the right to see that the public is treated fairly and honestly. It must, therefore, be permitted a reasonable amount of supervision and the determination of proper policies as to the content of advertisements published. These policies must be nondiscriminatory and fair.

The Commission, therefore, concludes that the complaint should be dismissed.

The Commission is further of the opinion and concludes that Complainant's "Petition To Set Aside Submission And Reopen Proceedings For The Taking Of Additional Evidence And Modification Of Complaint" should be denied.

It is, therefore,

ORDERED: 1. That Complainant's "Petition To Set Aside Submission And Reopen Proceedings For The Taking Of Additional Evidence And Modification Of Complaint" be, and the same is, hereby denied.

ORDERED: 2. That the complaint in Case No. 17,158 be, and the same is, hereby dismissed.

ORDERED: 3. That any objections not heretofore ruled on be, and they are, hereby overruled.

ORDERED: 4. That this Report and Order shall become effective on the 17th day of December, 1971, and the Secretary of the Commission shall serve a certified copy of same upon each interested party.

BY THE COMMISSION

[Signed]

Sam L. Manley
Secretary

(SEAL)

Jones, Chm., Fain, Reine,
and Mauze, CC., Concur.

Clark, C., Absent

Dated at Jefferson City, Missouri
this 7th day of December, 1971.

No. 72-C-743(2)—Filed: June 22, 1973

UNITED STATES DISTRICT COURT EASTERN DISTRICT OF MISSOURI EASTERN DIVISION

MARTIN MARKOWITZ,

PLAINTIFF

vs.

AMERICAN TELEPHONE AND TELEGRAPH COMPANY,
INC. and SOUTHWESTERN BELL TELEPHONE COMPANY,
a Missouri corporation,

Defendants

JUDGMENT

In accordance with the Memorandum and Order of the Court this day filed, which is incorporated in and made a part of this judgment;

It is hereby ORDERED and ADJUDGED that judgment be and is hereby entered in favor of defendants and against plaintiff dismissing plaintiff's complaint and all counts hereof.

/s/ William D. Runa
William D. Runa, Clerk
United States District Court

Entered by direction of the Court.

No. 72-C-743(2)

IN THE UNITED STATES DISTRICT COURT EASTERN DISTRICT OF MISSOURI EASTERN DIVISION

MARTIN MARKOWITZ,

Plaintiff,

vs.

AMERICAN TELEPHONE AND TELEGRAPH COMPANY,
INC. and SOUTHWESTERN BELL TELEPHONE COMPANY,
a Missouri corporation,

Defendants.

MEMORANDUM AND ORDER

Plaintiff, an operator of a private detective agency in the St. Louis area, sought to place advertisements in the Yellow Pages directories of Southwestern Bell Telephone Company beginning with the telephone directories of the year 1967. This action for monetary damages stems from those efforts.

The basic thrust of the complaint is that in each of the directory years commencing in 1967 defendants permitted plaintiff's competitors to use certain words and phrases in their Yellow Pages advertisements, the use of which words and phrases was denied to plaintiff, thereby discriminating against him to his damage. He seeks recovery on five theories, each of which is set forth in a separate count of the complaint.

Defendants have moved for summary judgment, the motion being premised on the contention that plaintiff is precluded from litigating the underlying factual issues in this Court under the doctrine of collateral estoppel, the facts having allegedly been determined adversely to plaintiff in a prior proceeding before the Missouri Public Service Commission.

On January 19, 1971, plaintiff filed a complaint with the Commission alleging discrimination against him by the Southwestern Bell Telephone Company in its Yellow Pages directories. On the basis of the complaint Southwestern Bell was ordered to answer the complaint, and thereafter an evidentiary hearing was held, at

which plaintiff was represented by counsel and personally testified. On December 7, 1971 the Commission filed its report and order dismissing the complaint on the merits, and thereafter on January 18, 1972, dismissed a further petition by plaintiff relating to the December 7th order. Plaintiff did not take an appeal or seek judicial review in the courts of the findings and order of the Commission adverse to him. The motion for summary judgment urges that since the order of the Commission was based on the ultimate fact finding that Southwestern Bell had not discriminated against plaintiff, the same factual issue may not again be litigated in this Court.¹

The doctrine of collateral estoppel is well established. The general principle of that doctrine is that a right, question, or fact directly put in issue and directly determined by a tribunal of competent jurisdiction may not be disputed in a subsequent action by the same parties and their privies, and that even if the second action is for a different cause of action, the right, question, or fact previously so determined must, as between the same parties and their privies, be taken as conclusively established.

In each instance in which the doctrine of collateral estoppel is relied on, "The question is whether an issue litigated in the earlier suit is determinative of some matter in controversy in the latter suit." To answer this question, "We must look to the pleadings making the issues, and examine the record to determine the questions essential to the decision of the former controversy." *Nelson v. Swing-A-Way Manufacturing Company*, 8 Cir., 266 F.2d 184, 187, which also noted that "(t)he doctrine of collateral estoppel applies to matters necessarily decided in the former judgment even if there is no specific finding or reference thereto."

That the Commission is an administrative body, not a court, does not affect the application of the doctrine. See *United States v. Utah Construction & Mining Co.*, 384 U.S. 394, 422. As the Supreme Court there stated (lc. 422), "When an administrative agency is acting in a judicial capacity and resolves disputed issues of fact properly before it, which the parties have had an adequate opportunity to litigate, the courts have not hesitated to apply *res judicata* to enforce repose," citing, inter alia, *Goldstein v. Doff*, 236 F.Supp. 730, affirmed 353 F.2d 484, cert. den. 383 U.S. 960, where collateral estoppel was applied to prevent relitigation of factual disputes resolved by an arbitrator.

There can be no doubt that in hearing plaintiff's complaint and adjudicating the merits thereof the Commission was acting in a judicial capacity. And the record conclusively establishes that an adequate opportunity was afforded the parties to litigate the factual issues involved in the complaint. In this situation, plaintiff's failure to appeal the adverse decision does not afford him any additional rights with respect to relitigating the facts.

Plaintiff suggests that the Commission did not have jurisdiction to determine the merits of his complaint. Plaintiff is hardly in a position to make this contention, having initiated the proceeding and submitted himself to the jurisdiction of the Commission. The very purpose of holding a hearing on the complaint was to ascertain whether the telephone company was guilty of discriminating against plaintiff by enforcing its advertising standards unfairly as to him. Had it found discrimination, the Commission could have entered an appropriate order to that effect. Otherwise, such a hearing would be an exercise in futility. Plaintiff cannot have it both ways. If there is jurisdiction to find dis-

crimination, there is jurisdiction to find the absence of discrimination. Whatever the finding, the parties are bound thereby. However, the issue is one of state law, and the jurisdiction of the Commission to hear and determine complaints such as plaintiff's is clear under *Videon Corporation v. Burton*, Mo. App., 369 S.W.2d 264, which fully considered the specific question and held that the Commission had jurisdiction to regulate advertising in classified directories and to adjudicate a complaint based on alleged discrimination in refusing to accept certain advertisements because of the content.

We next turn to the decisive question: Are the issues which were litigated before the Commission or necessarily decided by it determinative of the matters now in controversy? The complaint filed with the Commission and the testimony adduced by plaintiff charged in substance that Southwestern Bell applied its standards for advertising in the Yellow Pages directories in a manner discriminatory to him. Thus, the ultimate fact issue necessarily decided by the Commission was that of discrimination vel non.

The standards adopted by Southwestern Bell included one referred to as the "invasion of privacy" standard which reads: "Advertising copy stating or implying that wiretapping is employed should not be accepted. Equally unacceptable is the offer of electronic devices or of services involving the use of such devices which may cause the invasion of privacy by eavesdropping." This standard was first made applicable in the St. Louis area for the 1967 Yellow Pages directory, the one in which plaintiff first sought to place an advertisement. In the application of this standard the telephone company determined that detective agencies may not use the words "bugging" or "debugging" nor may they advertise the ability to place concealed listening devices or the ability to detect or remove such devices.

In his complaint before the Commission plaintiff contended that in 1967 he was refused the right to use the word "detection," a word which a competitor was permitted to use in his advertisement that year. The Commission found on the basis of the evidence that the telephone company had not refused to allow the plaintiff to use the word "detection" and would have permitted him to do so had he requested it with respect to the 1967 directory. This fact finding is binding on plaintiff.

In the following year (1968) the telephone company's construction of its "invasion of privacy" standard was made more stringent, so that detectives or private investigators were thereafter prohibited from advertising the ability to detect and remove electronic devices. This revised interpretation of the standard was based upon the conclusion which the St. Louis area directory personnel had reached that advertising the ability to detect and remove electronic devices was also, in effect, advertising the ability to place those same devices. As a result no advertisements for the St. Louis directory were accepted from anyone using the phrase "detection of electronic devices" or even the phrase "removal of electronic devices" which had appeared in plaintiff's 1967 advertisement. Up to this point therefore there was no basis in fact for a claim of discrimination, and the Commission so found.

The only other advertisement by a competitor of which plaintiff complained appeared in the 1969 directory. The facts as found in detail by the Commission disclosed that the publication of the advertisement complained of (which was violative of the "invasion of privacy" standard) was unquestionably the result of a good faith error or mistake. The improper advertisement was not permitted in the 1970 directory. The Commission further found that the plaintiff did not contract for the placement of any paid advertisements in the 1971 issue.

On the basis of all the evidence, the Commission found that the telephone company had not discriminated against plaintiff with respect to the permitted wording of his advertisements in applying its standards. In connection with the complaint before

¹ Defendants have also submitted undisputed affidavits disclosing that only customers who apply for and are currently being furnished with business telephone service are entitled to be listed in or apply for paid advertising in any Yellow Pages directory issued by the telephone company, and that as of January 10, 1972 the business telephone service theretofore furnished to plaintiff was terminated for non-payment of charges and that plaintiff has not since that date applied for or been furnished business telephone service or applied for any listing or paid advertising in any Yellow Pages directory issued by Southwestern Bell Telephone Company.

the Commission, plaintiff presented evidence that there were advertisements in the 1968, 1969 and 1970 Yellow Pages directories in Springfield and Kansas City which violated the "invasion of privacy" standard. Plaintiff was not in competition with detectives in those areas or in any other place outside the St. Louis area. The record before the Commission showed that different personnel were involved in applying the standards in various areas and that it took about three years for the telephone company to achieve uniformity for the Yellow Pages advertising by private detective agencies for the areas of Springfield, Kansas City and St. Louis.

Necessarily implicit in the ultimate finding of the Commission was that the foregoing facts did not constitute discrimination against plaintiff. The Commission stated, "It is clear from the evidence that [the Southwestern Bell Telephone Company] was making an effort to eliminate such advertising and further that this could not be accomplished at once in all three cities. In 1971 the Yellow Pages directories all conformed to [the telephone company's "invasion of privacy" standard]". Having found that the telephone company's standards as to the content of the advertisements were administered in non-discriminatory and fair manner, the complaint was ordered dismissed.

In our judgment, after a review of the record before the Commission, including the pleadings, the testimony, exhibits, briefs and findings, the underlying factual issue relating to plaintiff's complaint of discrimination on the part of the telephone company was determined adversely to plaintiff, and may not now be relitigated in the present action.

Plaintiff urges that all the Commission found or could have found was that the telephone company was not guilty of "unlawful" discriminatory conduct under Missouri law, so that he is now authorized to litigate his claims that such conduct constituted a violation of federal law. We do not agree. Whatever the theory on which plaintiff is proceeding, the facts themselves govern and it is those facts which the Commission determined in the complaint before it. Cf. *Engelhart v. Bell and Howell Company*, 327 F.2d 300, and see *Johnson v. Department of Water and Power of the City of Los Angeles*, 9 Cir., 450 F.2d 294, and *Edwards v. Vasek*, 8 Cir., 469 F.2d 294, 295. It has been well said that "a plaintiff cannot escape the effect of the adverse determination by clothing the claim in a different garb." The Commission found as a fact that there was no discrimination. It is that fact which plaintiff may not now dispute, whatever the legal theory of his subsequent claim.³

American Telephone and Telegraph Company, Inc. has been joined as a defendant on the theory that Southwestern Bell acted as its agent and under its direction. Our finding that the doctrine of collateral estoppel precludes plaintiff from litigating its claim against Southwestern Bell is equally applicable to the alleged principal, American Telephone and Telegraph Company, Inc.

Accordingly, IT IS HEREBY ORDERED that defendant's motion for summary judgment should be and it is hereby sustained and the Clerk is hereby ordered to enter judgment in favor of defendants and against plaintiff dismissing plaintiff's complaint and all counts thereof.

Dated this 22nd day of June, 1973.

[Signed] _____
UNITED STATES DISTRICT JUDGE

³ The federal law claims are contained in Counts II and III. Count II asserts that the alleged refusal of defendants to permit plaintiff to use the same words and phrases in his advertising as they allowed his competitors to use constituted a violation of Section 13(e), 15 U.S.C. The theory of Count IV is that such conduct denies plaintiff the equal protection of the laws in violation of his civil rights under Section 1983, 42 U.S.C. For present purposes we need not determine whether the alleged conduct of defendant would entitle plaintiff to relief under those federal law theories.

PROFESSOR BLAKEY: Our next witness will be Mr. John P. Linehan, a former FBI agent who is now a Professor at Seminole Junior College in Florida.

Dr. Linehan will give testimony on pre-1968 electronic surveillance and organized crime.

Dr. Linehan, will you please be sworn.

[Whereupon, John P. Linehan was sworn.]

TESTIMONY OF JOHN P. LINEHAN, PROFESSOR, SEMINOLE JUNIOR COLLEGE, FLORIDA

PROFESSOR BLAKEY: Would you state your name for the record, please?

MR. LINEHAN: John P. Linehan, L-i-n-e-h-a-n.

PROFESSOR BLAKEY: What is your present address?

MR. LINEHAN: 1566 Findlay Street, Daytona, Florida.

PROFESSOR BLAKEY: And your present occupation?

MR. LINEHAN: I am coordinator and instructor in a criminal justice program at the Seminole Junior College, Sanford, Florida.

PROFESSOR BLAKEY: Included among your courses, do you teach materials in organized crime?

MR. LINEHAN: Yes, sir, I do.

PROFESSOR BLAKEY: And how long have you taught those?

MR. LINEHAN: For three years, sir.

PROFESSOR BLAKEY: Prior to that time, where were you employed?

MR. LINEHAN: After leaving the FBI, I was employed by the Department of Law and Public Safety in New Jersey. I resigned from that and entered private practice in New York. And after my wife had a heart attack, we moved to Florida.

PROFESSOR BLAKEY: How long were you in the FBI?

MR. LINEHAN: Twenty-and-one-half years.

PROFESSOR BLAKEY: Would you tell us the nature of your assignments?

MR. LINEHAN: For 19 1/2 years of those 20 1/2, I worked on criminal matters. And for about five years of that time, from 1960, I worked in organized crime.

PROFESSOR BLAKEY: Where was your area of activity?

MR. LINEHAN: On the area of organized crime, it was out of the Newark Division.

PROFESSOR BLAKEY: After leaving the Federal Bureau of Investigation, were you employed as a special counsel to the Subcommittee on Criminal Laws and Procedures of the United States Senate?

MR. LINEHAN: Yes, sir, I was. I was employed in the fall of 1969 through the spring of 1970 as special counsel for that committee.

PROFESSOR BLAKEY: Would you indicate what the nature of that employment was?

MR. LINEHAN: I was asked to review the tapes of Sam DeCavalcante. He was the head of the New Jersey family of organized crime. And the tapes had been made public due to the fact that he had been indicted in connection with a criminal matter and his defense attorney, Mr. Franzblau, made an accusation that the tapes were obtained by an unauthorized device—been made available.

PROFESSOR BLAKEY: Were those tapes subsequently made a matter of public record in that case?

MR. LINEHAN: Yes, because when Mr. Sachs, then U.S. Attorney, brought in the volumes to the court, Mr. Franzblau had neglected to ask the court for the examination and then sealing, and so they were entered into the court clerk's record and became public records.

PROFESSOR BLAKEY: And they are now available to anyone who wants to read them?

MR. LINEHAN: Yes.

PROFESSOR BLAKEY: Would you describe for us in general terms the nature of those documents?

MR. LINEHAN: The documents consisted of tapes that were made—

PROFESSOR BLAKEY: Do you mean tapes?

MR. LINEHAN: The transcripts, I should say—transcripts made from the tapes. And the transcripts were reviewed by the investigative clerks and then reviewed by the analytical agents who passed it off. They were then sent to the case agent involved in that particular matter. And the summary contains—

PROFESSOR BLAKEY: It is my understanding that the documents are logs, administrative documents, and actual transcripts?

MR. LINEHAN: Yes.

PROFESSOR BLAKEY: Would you tell us what the logs were?

MR. LINEHAN: The logs, Professor Blakey, consisted of the date, the time, and the initial of the person who was on the tape at that particular time.

For example, one starts at 10:08 a.m. on Sunday, February 11, 1962. And any activity that comes over is logged in as to the time and the initial of the person who is involved in it.

PROFESSOR BLAKEY: What was the purpose of this log entry by the investigative clerk?

MR. LINEHAN: That would be for a complete record of the activity at that particular time.

If, for example, he were away on a fishing trip or something like that, there'd be no activity at that time.

PROFESSOR BLAKEY: When the investigative clerk entered an occurrence into the log, was a tape recorder also simultaneously running?

MR. LINEHAN: Oh, yes. The tape recorder was available because the investigative clerk might, for example, put down "not clear" or "garbled," or possibly it might be in a foreign language, in which event it was then examined by an agent who was conversant with that particular language.

PROFESSOR BLAKEY: Was there any attempt by the clerk to be full and complete in entering the logs, or were they just sort of an index for the tapes?

MR. LINEHAN: Oh, no, they were fully complete in the sense of "unknown person enters the office and moves around."

PROFESSOR BLAKEY: I take it they were accurate but they didn't purport to repeat everything that was overheard.

MR. LINEHAN: I'm sorry. I misunderstood you. They are not in all respects verbatim, but only verbatim when it is pertinent and material.

PROFESSOR BLAKEY: If I understand your procedure correctly, at various times the case agent would come in and, using the logs, would examine the tapes themselves; is that correct?

MR. LINEHAN: That is right.

PROFESSOR BLAKEY: And would he then order some or all of the tapes transcribed?

MR. LINEHAN: That is right.

PROFESSOR BLAKEY: When the case was transcribed, would he transcribe fully and accurately?

MR. LINEHAN: If it was deemed important, it would be verbatim as it was at that particular point.

PROFESSOR BLAKEY: Did the case agent cause to be prepared certain administrative memoranda commenting on the transcripts?

MR. LINEHAN: Yes, sir. Administrative memorandum is where the case agent would review it and interpret as best he could at that particular time what was meant, and try to interpret what was meant by using certain expressions, such as foreign words, summing up an activity.

PROFESSOR BLAKEY: Would it be fair to describe the administrative memorandum as a kind of contemporaneous memorandum by the people of what they thought was going on?

MR. LINEHAN: Yes, sir. It was contemporaneous in the sense it was done either the same day or the following day, depending on the time of the intercept.

PROFESSOR BLAKEY: Now, in addition, the files contain airtels and radiograms. Would you describe what they are?

MR. LINEHAN: Well, for the sake of economy, we used airtels. They were handled with priority just under that of a teletype.

A radiogram, as you can well imagine, is one that had been sent by radiogram.

PROFESSOR BLAKEY: What was the nature of an airtel or radiogram? What would they contain?

MR. LINEHAN: It usually would contain a summary of the activity deemed pertinent for that particular day. And if there were a number of activities, on occasion you'd have as many as three or four airtels out of the same day's activities.

PROFESSOR BLAKEY: Did the airtels contain material in addition to that which was heard over the electronic surveillance?

MR. LINEHAN: Yes, sir. The airtel would set forth what the verbatim appeared to be and might incorporate an administrative summary of the agent, explaining why and what he had to do.

And occasionally they were sent to more than one area.

PROFESSOR BLAKEY: Now, the materials that were generally called the DeCavalcante papers contained—am I correct—logs, transcripts, airtels, and radiograms in which Mr. DeCavalcante himself participated?

MR. LINEHAN: That is right.

PROFESSOR BLAKEY: How many electronic devices were actually involved?

MR. LINEHAN: In the DeCavalcante papers there were two devices. The original one was on Angelo Bruno in Philadelphia in early '62. The DeCavalcante installation did not go into effect until September of 1964 and continued to some date in 1965 when President Johnson ordered all installations terminated.

PROFESSOR BLAKEY: Mr. Linehan, would you indicate for the record what it is that you did to these documents?

MR. LINEHAN: The 2300 pages of these transcripts were reviewed by me, and I tried to interpret as best I could who the unknown person would be by the reference to him or the nickname involved. Because we had found through experience that they didn't always refer to the person by the same name in different areas. It might be a different nickname in different places.

PROFESSOR BLAKEY: In connection with this, did you paginate the document separately?

MR. LINEHAN: Yes, sir. We started with the number of pages of the documents and went right through the 2300.

PROFESSOR BLAKEY: Approximately what period of time did you spend analyzing these documents?

MR. LINEHAN: About four or five months part time. For the first couple of months, I did it full time until I suddenly found out I wasn't teaching part time; I was teaching full time and running a program, and I cut down on my time.

PROFESSOR BLAKEY: As a result of that effort, have you ever prepared a report?

MR. LINEHAN: Yes, sir, I have.

PROFESSOR BLAKEY: Without objection, I'd like to enter the report in the record at this point and note that it consists of a table of contents, an analysis of tapes, and an appendix at the conclusion by name.

[The documents referred to follow.]

TABLE OF CONTENTS

I. ORGANIZED CRIME

II. INTERNAL STRUCTURE

III. TWO ASPECTS OF ORGANIZED CRIME THAT MAKE IT UNIQUE

IV. THE COMMISSION

V. SAMUEL RIZZO DeCAVALCANTE AKA "SAM THE PLUMBER"

a. SAM'S ATTORNEY'S MOTION REQUESTING TRANSCRIPTS

b. U.S. ATTORNEY PRODUCED 2300 PAGES OF TRANSCRIPTS

1. THAT THERE IS AN ORGANIZATION CALLED LA COSA NOSTRA
2. THAT COSA NOSTRA IS HEADED BY BODY CALLED "THE COMMISSION."
3. THAT THE FAMILIES ARE STAFFED BY CAPOREGIME, THAT IS CAPTAIN, AND THE CAPTAINS ARE APPOINTED BY AND CAN BE REMOVED BY THE BOSS
4. THAT THE COMMISSION CAN REPLACE A BOSS OF A FAMILY AND THE FAMILY REPRESENTATIVES
5. THAT FAMILIES ARE STAFFED BY UNDERBOSSSES, AS WELL AS CAPOREGIMES AND SOLDIERS
6. THAT THE COMMISSION MUST APPROVE NEW MEMBERS
7. THAT MEMBERS TRANSFER FROM FAMILY TO FAMILY
8. THAT MEMBERS ARE ORDERED TO MURDER
9. THAT THE BOSS OF A FAMILY IS INTERESTED IN MACHINES TO DISPOSE OF BODIES
10. THAT MEMBERS OF A FAMILY MUST FOLLOW COSA NOSTRA PROTOCOL
11. THAT THE BOSS OF THE FAMILY APPROVES DESTRUCTION OF A DEBTOR'S BUILDING BY ARSON IN ORDER TO COLLECT THE INSURANCE AND PAY THE SHYLOCK LOAN BUT "DOES NOT WANT TO KNOW"
12. THAT THE BOSS HAS POLITICAL CONTACTS WHO ARE FRIENDLY AND DO FAVORS FOR THE BOSS AND FOR THE FAMILY
13. THAT THE BOSS AND FAMILY MEMBERS HAD CONTACTS WITH LAW ENFORCEMENT PEOPLE AT ALL LEVELS WHO COULD AND DID DO FAVORS FOR THE BOSS AND HIS FAMILY

14. THAT THE BOSS OF THE FAMILY CONTROLS SOME UNIONS AND HAS WORKING AGREEMENTS WITH OTHER UNIONS AND USES THE UNIONS TO GET PAYOFFS AND OTHER ADVANTAGES FOR HIMSELF AND/OR HIS FAMILY
15. THAT FAMILY BOSSES ARE VERY MUCH INTERESTED IN GARBAGE
16. THAT THE BOSS OF THE FAMILY HAS CONTACTS WITH LEGITIMATE BUSINESS WORLD WHICH PERMIT HIM TO USE INFLUENCE IN PLACING PEOPLE IN POSITIONS
17. THAT THE BOSS AND MEMBERS OF A FAMILY ARE ENGAGED IN GAMBLING
18. THAT THE BOSS AND MEMBERS OF A FAMILY ARE ENGAGED IN LOAN SHARKING (SHYLOCKING)
19. THAT THE BOSS TRIES TO INSULATE HIMSELF FROM POSSIBLE CRIMINAL PROSECUTION—IS CONCERNED ABOUT SECURITY

ORGANIZED CRIME, HOW IT OPERATES—AS DISCLOSED BY SAMUEL RIZZO DeCAVALCANTE—A LEADER IN ORGANIZED CRIME.

The President's Commission on Law Enforcement and Administration of Justice had this to say about organized crime: "In many ways organized crime is the most sinister kind of crime in America. The men who control it have become rich and powerful by encouraging the needy to gamble, by luring the troubled to destroy themselves with drugs, by extorting the profits of honest and hard working businessmen, by collecting usury from those in financial plight, by maiming or murdering those who oppose them, bribing those who are sworn to destroy them. Organized crime is not merely a few preying upon a few. In a very real sense, it is dedicated to subverting not only American Institutions but the very decency and integrity that are the most cherished attributes of a free society. As the leaders of La Cosa Nostra and their racketeering allies pursue their conspiracy unmolested in open and continuance defiance of the law, they preach a sermon that all too many Americans heed: 'The Government is for sale; lawlessness is the road to wealth; honesty is a pitfall and morality a trap for suckers'."

Today, the corps of the organized crime in the United States consists of twenty-four groups operating as criminal cartels in large cities across the Nation. Their membership is exclusively of Italian descent, they are in frequent communication with each other and their smooth functioning is assured by national body of overseers.

In 1966, J. Edgar Hoover told a House of Representatives Appropriations Committee: "The Cosa Nostra is the largest organization of the criminal underworld in this country, very closely organized and strictly disciplined. They have committed almost every crime under the sun."

INTERNAL STRUCTURE

Each of the twenty-four groups is known as a "family" with membership varying from as many as seven hundred men to as few as twenty. Most cities with organized crime have only one family; New York City has five families.

Each family or borgata is headed by one man, the "Boss", whose primary functions are maintaining order within the family and maximizing profits. Subject only to the possibility of being overruled by the national advisory group called the Commission, the Boss's authority in all matters relating to his family is absolute.

Beneath each Boss is an Underboss, the Vice-President or Deputy Director of the family. He collects information for the Boss; he relays messages to him and passes the Boss's instruc-

tions down to his own underlings. In the absence of the Boss, the Underboss acts for him.

On the same level as the Underboss, rating in a staff capacity, is the Consigliere who is a counselor or advisor. Often an older member of the family who has partially retired from a career in crime, he gives advice to family members, including the Boss and Underboss and he enjoys considerable influence and power.

Below the level of the underboss are the caporegime, some of whom served as buffers between the top members of the family and the lower-echelon personnel. To maintain their insulation from the police, the leaders of the hierarchy (particularly the Boss) avoid direct communications with the workers. All commands, information, complaints and money flow back and forth through a trusted go between. A Caporegima fulfilling this buffer capacity, however, unlike the Boss does not make decisions or assume any of the authority of his Boss.

Other "caporegime" serve as chief of operating units. The number of men supervised in each unit varies with the size and activities of particular families. Often a Caporegima has one or two associates who work closely with him, bringing orders, information and money to the men who belong to his unit. From a business standpoint the caporegima is an analogous to plant supervisor or sales manager. Members of the family at the lowest level are the "Soldati", the soldiers or "button men" who report to the caporegime. A soldier may operate a particular illicit enterprise, for example a loan sharking operation, a dice game, a lottery, a book making operation, a smuggling operation, on a commission basis or he may "own" the enterprise; a portion of its profit to the organization in return to operate. Partnerships are common between two or more soldiers and between soldiers and men in the hierarchy. Some soldiers and most echelon family members have interest in more than one business.

Beneath the soldiers in the hierarchy are a large number of employees and commissioned agents who are members of the family and are not necessarily of Italian descent. They do most of the actual work in the various Enterprises. They have no buffers or other insulation from law. They take bets, drive trucks, answer phones, sell narcotics, tend stills, work in the legitimate businesses. For example, in a major lottery business in Chicago that operated in Negro neighborhoods the workers were Negroes; the bankers of the lottery operations were Japanese-American; but the game including the banking operation was licensed for fee by a family member.

Two aspects of organized crime that characterize it as a unique form of criminal activity are:

1. Element of Corruption
2. Element of Enforcement, necessary for the maintenance of internal discipline and the regularity of business transactions.

The organized crime groups are believed to contain one or more fixed positions for "Enforcers" to maintain organizational integrity by arranging for the maiming and killing of recalcitrant members. The "Corrupter's" function is to establish relationships with those public officials and other influential persons whose assistance is necessary to achieve the organization's goals.

THE "COMMISSION"

The highest body of the twenty-four families is the "Commission". This body serves as a combination Legislative, Supreme Court, Board of Directors, and Arbitration Board; its principal functions are Judicial. Families look to the Commission as the ultimate authority on organizational and jurisdictional disputes. It is composed of the Bosses of the nation's most powerful families but has authority over all other families. The composition of the "Commission" varies from nine to twelve men. According to current information there are presently nine families represented, five from New York City and one each from Philadelphia, Buffalo, Detroit, and Chicago.

SIMONE RIZZO DeCAVALCANTE
also known as Samuel Rizzo DeCavalcante,
Sam Rizzo, Samuel DeCavalcante,
"Sam the Plumber".

Samuel Rizzo DeCavalcante is the head Boss of one of the twenty-four families Cosa Nostra. He became Boss of the family after the natural death of Nick Delmore,¹ Feb. 1964.

March 21st, 1968, DeCavalcante and others were indicted for conspiracy to violate and by causing interstate transportation in aid of racketeering enterprises. On April 16th, 1968, in a reply to a defense motion for a bill of particulars requesting transcripts of unlawfully accepted communications, the Government filed two memoranda with the Court which admitted that electronic surveillance of DeCavalcante and others had occurred, giving the dates and locations, but claiming that none of the monitored conversations had any relevancy to the indictment and that none would be used as evidence in any manner. On June 10th, 1969, the Government filed the thirteen volumes of transcripts in a Bill of Particulars, which made them a matter of public record. These transcripts comprise approximately twenty-three hundred pages.

The Government in its memorandum had advised the Federal Court and the defendant Samuel Rizzo DeCavalcante, that the Federal Bureau of Investigation had installed a microphone at the Kenworth Corp., 21 North Michigan Ave., Kenilworth, New Jersey, the place of business of defendant, DeCavalcante, where he and others frequently met. This microphone was in operation from August 1964 until July 1965 and during this period, various conversations of Samuel Rizzo DeCavalcante were monitored by employees of the Federal Bureau of Investigation.

It was believed by the Federal Bureau of Investigation that this place of business was being utilized for purposes connected with Organized Crime. The Federal Bureau of Investigation, acting on the basis of authorization by the Department of Justice approved the microphone installation here in question.

These transcripts are now a matter of public record. A review of the transcripts has established:

1. That there is an organization called La Cosa Nostra.

A. On February 11, 1962, Samuel Rizzo DeCavalcante visited Angelo Bruno,² Boss of the Philadelphia family. Ignatius Denaro,³ also known as Gnatz, a close associate of Bruno's was present.

Bruno stated: "It's better that they ask do you know Angelo? Cosa Nostra, Cosa Nostra "I don't know nothing about Micky Russo." (Page 77)

B. Bruno: "Listen, before I was amico nostro (term used to identify person as a member of Cosa Nostra. When a person is initiated into Cosa Nostra, he is described as 'having been made') there was a fellow who used to come to my house with his wife. Mr. Maggio⁴ came to my house one time, he had a proposal from Cosa Nostra. He said, 'don't let her come in here no more.' That woman never came into my house again." (Page 77)

C. In discussion of the Majuri wedding, Louis Larasso⁵ told La Cosa Nostra Boss, Samuel Rizzo DeCavalcante, the following: "John 'Sonny' Franzese⁶ introduced Larasso to Vincent 'Vinnie' Gagliardi who was seated at the Franzese table. Larasso recognized Gagliardi as an old army buddy. He said that Gagliardi was clearly identified as La Cosa Nostra member in Joseph Colombo⁷ family. He was described as an Organizer for the teamsters union with responsibility for 'half the state of New Jersey' although his residence was said to be Brooklyn, New York." (Newark Radiogram June 3, 1965) (Pg. 1964)

D. On June 16, 1965, Samuel Rizzo DeCavalcante greeted an unnamed male. They discussed the funeral of Ciconia from the Trenton-Bordentown, New Jersey area who had just been buried, having died of a heart attack. Tony and the other male are from a different family.

DeCavalcante: . . . "There is no difference between you and Joe and our people. When you people are here, you are respected like our people . . . Respect for you belonging to another family, you don't have to tell me anything. If you need money, we will give it to you, we will respect you as an Amico Nostro . . . Cosa Nostra is Cosa Nostra. I can only speak for my people, but not for anyone else. When you call the family for your own intention, an Amico Nostro is an Amico Nostro. If he belongs here or there it doesn't mean a thing. If you give me preference, I will also give you preference." (New York Airtel to Washington dated 7/2/65) (Pgs. 2194, 2195)

2. That Cosa Nostra is headed by body called "The Commission".

A. On February 11, 1962, Angelo Bruno,² Boss of the Philadelphia family, and lieutenant Ignatius Denaro³ were visited by Samuel DeCavalcante who at that time was not yet the Boss of his family. He was "a soldier". DeCavalcante and James Christy, also known as Jimmy Christy, Jimmy Goia, were partners in a numbers operation in Bristol, Pennsylvania. They had difficulties about money in connection with this operation Jimmy is a member of the Philadelphia family. DeCavalcante is not a member of this family. He has gone to Bruno to discuss his problem. Bruno advised DeCavalcante that he would merely advise, pointing out that it was up to DeCavalcante and Jimmy to resolve their problems. If they did not resolve their problems they would have to present their sides of the story to the Arguimendo which is an "arguing body".

Angelo Bruno speaking: "I don't wanna to go, you understand, if it goes to 'Arguimendo', I represent Jimmy whether I want to or not and so does Denaro. You understand we have to represent him, and we have to represent him to the best of our ability without lying and without taking advantage of you. Now, if we go to their 'Arguimendo', you understand and your representando is there and I am there and let's say a few other representandos are there because he ain't going to make the decision and I ain't going to make the decision. Other people are going to make the decision. You're right, if we can't get together, it has to go further, it goes out of our hands. It can't just lay like that, it's got to go out of our hands. When it goes out of our hands then they make the decision." (Pg. 22-23)

Continuing this discussion of the numbers operation.

Angelo Bruno says: "Gnatz, he don't have to accept anything, he could say well I refuse to accept it. He's got to prove that he's lost that much money and it's a hard thing to prove, because the books say only \$5,000.00. Not only that but from time to time the books were out of there, Now this story that he lost the money in the house book, that's a story that if Sam himself says it, I wouldn't believe it myself or his experience. But this is not like in Trenton. Now if it goes to the Commission, the Commission says you're stuck \$11,000.00 Sam".

DeCavalcante: "Forget about it."

Bruno: "You say you stuck 50, he stuck 11. You both stuck the same thing, you can't prove you are stuck for money. I don't know what they would say, they are liable to say anything, I don't know what they are going to say."

DeCavalcante: "Ange, but who wants it to go to headquarters."

Denaro: "He's going to insist, he's going to say he's stuck all the time."

DeCavalcante: "He's not stuck all the time because, see, I gave him the account." (Pg. 89)

During this discussion of DeCavalcante's problem with Jimmy the word *Udienza* was used. This word is used to describe the situation where an amico nostro is discussing a matter with his family's caporegima. (Pg. 85)

B. In August 1964 Samuel Rizzo DeCavalcante was acting as intermediary in a dispute between Joseph Bonanno,⁸ also known as Joe Bananas, in the Cosa Nostra Commission.

A dispute had developed in the Bonanno family centering around Gasparino DeGregorio,⁹ who held the position of Caporegima in the family. Because of Gasparino's actions, unknown at this time, Bonanno had placed him "on the shelf," that is, ostracized him from the Bonanno family.

DeCavalcante, together with Angelo Bruno and Joseph Zerilli,¹⁰ had met with Bill Bonanno, son of Joseph Bonanno and Johnny Burns,¹¹ true name John Morales, Bonanno's Underboss. They told Bonanno and Morales that there were several important matters the Commission wished to discuss with Joe Bonanno.

Joseph Bonanno refused to accept this message as official and ignored the Commission's summonses. It should be noted the significance was placed on official notices being delivered by three people, which suggests that this is an established procedure in Cosa Nostra.

On September 19, 1964 DeCavalcante met with Joseph Bonanno and pleaded with Bonanno to go with him to the Commission so that the problem could be resolved peacefully. Bonanno declined.

As a result of this final rebuff, the Commission unanimously, that is the remaining eight members of the Commission, voted to withdraw recognition of Joseph Bonanno as a Boss of a family. Although acknowledged to be a drastic step, the Commission wanted it made plain that they bore no illwill toward the family as a whole nor had they any quarrel with any of Bonanno's administration, which is understood to include all the Caporegimas of the Bonanno family. The Commission would be content with the removal of Joseph Bonanno⁸ as the Boss, Johnny Burns¹¹ as the Underboss and Bill Bonanno, the son of Joseph Bonanno, as the consiglieri. They also noted that these men were in no personal danger, providing that they took no action against anyone else.

On September 23, 1964 DeCavalcante discussed the Bonanno situation with Gerardo Catena,¹² Underboss of the Genovese family. Catena said that he believed DeCavalcante had gone far enough with this matter and DeCavalcante should now "divorce himself from it". Catena made it clear that the Commission will not make any further concessions. (Newark Airtel to Washington dated Sept. 24, 1964)

C. On September 21, 1964 DeCavalcante met with Joseph Arthur Zicarelli¹³ also known as Joe Bayonne, to discuss the Bonanno family problem. Zicarelli is a soldier in the Bonanno family.

DeCavalcante told Zicarelli that the Commission was formed by people, all Bosses, who have given the Commission the right to supercede any Boss. Joe Bonanno knows that for he made the rules. Now the Commission thinks, "Here this guy's a Boss and he is not treating his people right." (Newark Airtel to Washington dated Sept. 25, 1964) (pg. 263)

Continuing the discussion of the relationship between the Commission and the family, Joseph Zicarelli and Sam DeCavalcante went on.

The names will be mentioned first and the quotation assigned to them following:

DeCavalcante: "The Commission also knows that Bonanno's family administration is under Joe Bonanno's orders—but the Commission supercedes any Boss."

Zicarelli: "He ought to know that."

DeCavalcante: "Better than anybody."

Zicarelli: "But, do they supercede any Boss as far as coming into your family."

DeCavalcante: "They can go into your immediate family."

Zicarelli: "This don't make sense to me if that's the way it is, I don't like it. Who the hell am I to even say it, now we're talking between you and I."

Zicarelli: "Let's say the Commission wants you, Sam, and they tell you this and this and this, but who are they to come into your house and tell your family this ain't right."

DeCavalcante: "Suppose you're being mistreated for no reason."

Zicarelli: "That's my business with my family why should I go to the Commission?"

DeCavalcante: "And there's nothing you could do; you can't fight the boss—but the Bosses gave the right to the Commission.—The Commission can go against it. See in Magliocco's¹⁴ family they had trouble in there—the Commission went in there and took the family over when Joe Profaci¹⁵ died, Joe Magliocco took over as Boss. They threw him right out saying 'Who the hell are you to take over a borgata?' He's lucky they did not kill him and Joe Bonanno⁸ knows this. When we had trouble in our outfit, they came right in. You people belong to the Commission until this is straightened out. They did the same thing in Pittsburgh, they made the Boss, John LaRocca,¹⁶ step down."

DeCavalcante: "They can supercede any Boss and go into your immediate family." (Newark Airtel to Washington dated 9/25/64) (pgs. 273-274-275)

D. Later on DeCavalcante, in another discussion with Zicarelli,¹³ discussed the strength of the Commission.

DeCavalcante: "Joe you don't know the strength of the Commission. As long as I am doing the right thing with my people and they are satisfied, the Commission has no jurisdiction to start anything. They can say 'listen we make this many laws'; they make lots of them but they can't mix in. When there's trouble in an outfit or when the head of the outfit is doing the wrong thing, you understand what I mean? Even if your Caporegima said 'no', he's your Boss you would have to go, if they called you, and it's the same thing, the Commission is his Boss, not individually but as a Commission."

(Newark Airtel to Washington dated Dec. 23, 1964) (Pgs. 865-867)

3. That the families are staffed by Caporegime, that is Captain, and the Captains are appointed by the Boss and can be removed by him.

A. On December 23, 1964 Joseph Notaro,¹⁷ Vito DeFilippo,¹⁸ and Joseph Zicarelli¹³ visited Samuel DeCavalcante. Notaro stated that the purpose of the visit with DeCavalcante was to bring him up to date concerning the Bonanno family dispute.

He stated: "I have Joe Bonanno,⁸ Johnny Morales,¹¹ Bill Bonanno on my hands; in other words we have a committee of four of which I am chairman. We have had a meeting and he, Joe Bonanno, resigned rather than see it go any further effective whatever date I tell him."

Notaro stated the meeting was held where he had been staying and the meeting lasted until 7:00 A.M. He added that four Captains had been on the "other side". Notaro reported that Bonanno said at the meeting that rather than have this continue and to avoid bloodshed he was resigning. Bonanno then appointed the four man committee. Notaro added that when the meeting broke up two of the committee Smitty D'Angelo¹⁹ and John Aquaro,²⁰ were sent to Angelo Caruso's²¹ house to explain what had taken place. Caruso was sorry to hear that Bonanno had resigned, according to Notaro. Notaro added that at a meeting the committee decided that all Captains would remain at least until a new Boss is elected. A new Boss would have authority to remove any Captain he does not want. He stated that a discussion was held at the meeting concerning procedure for electing a new Boss. At this meeting, according to Notaro, Gasparino DeGregorio⁹ said, "Well all right, these nine committeemen will notify the men that we are all in accord and to return to their Captains", and that's the way we left off. Notaro added they were going to contact the Commission and notify them that we had banded together and Gaspar indicated the Commission would be notified in one hour.

DeCavalcante asked Notaro; "How long you a friend of ours, Joe?" Notaro replied, "Ten years."

Sam DeCavalcante assured Notaro that his judgment is as good as those who have been members forty years.

Notaro went on to relate that the Captains who were at the last meeting with Joe Bonanno were Smitty D'Angelo,¹⁹ John Aquaro,²⁰ Johnny Burns,¹¹ true name Morales, Bill Bonanno, and Charlie Battaglia,²² from Arizona, Fran Labruzzo,²³ a Caporegima who was representing Montreal. He explained that Arizona was a decina belonging to the family because Bonanno was a Boss living there, otherwise this decina would belong to Colorado, Texas, or California.

(Newark Airtel to Washington dated 12/28/64) (Pgs. 897-901)

B. On May 7, 1964, Samuel DeCavalcante met with Gene Catena,²⁴ brother and chief Lieutenant of Gerardo Catena,¹² and discussed the DeCavalcante family. Gene Catena asked: "How many Caporegimes you got?"

DeCavalcante replied: "No Caporegimes. We got thirty-one or thirty-two soldiers. Most of them are old people who ain't making much. Those making money give me one third. Say one makes \$600.00, then he gives me \$200.00 and I don't split with nobody else."

Catena: "I'm a Caporegime who's always available. My people know where to find me or where or how they can reach me." (Newark Airtel to Washington dated 5/14/64) (Pg. 122)

C. On June 1, 1965, Samuel DeCavalcante told John Riggi,²⁵ his Caporegima, that he was thinking of taking Joe Sferra's²⁷ Union position away from him and putting Riggi in his place. DeCavalcante told Riggi, that if he takes the job, then his only responsibility will be to keep the "amico nos" in the union working. DeCavalcante added that he had sent his Underboss, Frank Majuri,²⁶ to see Sferra²⁷ and find out what happened to him when he was put in the hospital, but Sferra refused to discuss what happened to him.

He also told Riggi that he was to see members of the DeCavalcante family and tell them not to see Sferra on DeCavalcante's orders. DeCavalcante said he was going to put the chill on Sferra because of Sferra's obvious lack of respect and courtesy. (Pg. 2004)

D. On June 4, 1965, Lou Larasso,⁵ his Caporegima, contacted Sam DeCavalcante and DeCavalcante informed Larasso of his decision to remove Joe Sferra²⁷ "from everything". DeCavalcante said: "The only reason for doing this is because Sferra has been inattentive to his responsibility for keeping 'our people' working."

Larasso asked: "Are you taking him off of Caporegima too?"

DeCavalcante replied: "Yeah."

DeCavalcante emphasized that Sferra is still to be treated with respect since he is still "a friend of ours". DeCavalcante said that he told Sferra "I like you but I like our people better than you. You are just one of 30 people. And I'm not going to do an injustice to thirty people on account of you". (Pg. 2020)

E. On June 10, 1965, Mike Puglia²⁸ told Samuel DeCavalcante that he had advised Joe LaSelva²⁹ that he could not attend the family meeting on June 6th at Ange and Min's Restaurant, Kenilworth, N.J.

DeCavalcante said the purpose of this meeting was to announce to the hierarchy of the family that Joseph Sferra²⁷ had been removed as Caporegima and that Paul Farina³⁰ had been appointed in his stead. (Pg. 2116)

4. That the Commission can replace a Boss of a family and the family representatives.

A. On September 3, 1964, Samuel DeCavalcante conversed with Frank Majuri,²⁶ his Underboss. DeCavalcante indicated that he had been attending meetings with the Commission members or with the Commission itself and The Commission had under consideration a move to displace Joseph Bonanno⁸ and possibly his representatives from the Commission. DeCavalcante related that he had a meeting recently with Sam Mooney,³¹ true name Samuel Giancana, from Chicago about this matter. DeCavalcante told Majuri that he had been used as an intermediary between the Commission and Bonanno, but that Bonanno had

failed to heed his advice and had not presented himself before the Commission as ordered. He indicated that aligned against Bonanno are Mooney,³¹ Thomas Luchese,⁵² Carl Gambino,³³ Joe Colombo,⁷ Angelo Bruno,² and Jerry Catena.¹² Majuri and DeCavalcante agreed that the situation is worsening. (Newark Radiogram to Washington dated 9/11/64) (Pgs. 188-189)

On September 21, 1964, Samuel DeCavalcante met Joseph Zicarelli,¹³ also known as Joe Bayonne, and discussed the Joseph Bonanno⁸ dispute with the Commission. DeCavalcante said the Commission does not recognize Joe Bonanno as the Boss anymore. He said that he told Joe Notaro¹⁷ that the administration should know that the Commission has got nothing against any of you fellows. They respect all you people as friends of ours, but they will not recognize Joe Bonanno, his son Salvatore Vincent Bonanno, also known as Bill, and Johnny Burns,¹¹ true name John Morales. DeCavalcante further said that the Commission has no intention of hurting anybody but Joe Bonanno better not get any intention of hurting anybody either.

DeCavalcante added that the Commission was formed by people—all Bosses—who have given the Commission the right to supercede any Boss. Joe Bonanno knows that! He made the rules! Now, the Commission thinks, "Here this guy's a Boss and he's not treating his people right—"

DeCavalcante said that Joseph Bonanno made a bad move—he put Gasparino DiGregorio,⁹ he's a Caporegima, he put him on the shelf with the "amico nos". He said that Gasparino is under the protection of the Commission. He then asked Bayonne if Bonanno puts this guy on the shelf, why shouldn't the Commission put Joe Bonanno on the shelf, do you understand?

DeCavalcante said that Joe Bonanno tried to move in, into California. He tried to commit a tragedy over there so that his kid could take over in California. The Commission chased him out of California but he was trying.

In reply to Bayonne's question as to when Bonanno was going to take over California, DeCavalcante replied that this happened a few years ago when Billy Bonanno moved into California with forty men, they were trying to take over Stammano's outfit.

DeCavalcante said: "His own Uncle, who is the most respected of the Commission, Stefano Magaddino,³⁴ has pleaded with him to come up and see him."

DeCavalcante added that Magaddino cried to him saying that everyone says that Bonanno's a nice guy but that he, Magaddino, had sent for him and Bonanno did not know if Magaddino needed Bonanno to save his neck but Bonanno did not answer his call or go see him.

DeCavalcante then said: "That's why the Commission feels bad because they know that Bonanno lied to them, namely his family. The Commission wants the family to know the truth, then decide if they still want Bonanno, but the administration of the family did not show up to meet with the Commission, for it was acting under Joe Bonanno's orders."

DeCavalcante pointed out that the Commission supercedes any Boss.

By way of illustration DeCavalcante stated: "See in Magliocco's¹⁴ family they had trouble in there. When Joe Profaci¹⁵ died, Joe Magliocco took over as Boss. The Commission went in there and took the family over. They threw Magliocco right out. 'Who the hell are you to take over a borgata?' Magliocco's lucky they did not kill him and Signor Bonanno knows this. When we had trouble in our family, they came right in. 'You people belong to the Commission until this is straightened out'. They done the same thing in Pittsburgh. They made the Boss John"

Bayonne interrupts: "LaRocca".¹⁶

DeCavalcante: "LaRocca, made him step down; it's all straightened out now but they made LaRocca take orders from the Commission until everything was straightened out." (Newark Airtel to Washington dated 9/25/64) (Pgs. 261-276)

5. That Families are staffed by Underbosses, as well as Caporegimes and soldiers.

A. On June 10, 1965, Sam DeCavalcante and Joseph Arthur Zicarelli,¹³ also known as Jos Bayonne discussed family organization.

Joe Zicarelli said that Gaspar DiGregorio⁹ had told him that he, Gaspar, was the new Boss of the family of which Joe Bayonne is a member. He also said that Mike Sabella³⁵ is Joe Bayonne's new Caporegima. (Pg. 2086)

DiGregorio said that Skinny Pete is his Underboss.

Sam DeCavalcante introduced Joe Bayonne to Mickey Poole,²⁸ whom he described as his "Caporegima from Connecticut".

DeCavalcante advised Poole that he had removed Joe Sferra²⁷ as Caporegima and had put in Paul Farina³⁰ as Caporegima. He pointed out that Sferra is still a "Cosa Nostra" member. (Pg. 2089)

Joe LaSelva²⁹ is DeCavalcante's Underboss in Connecticut. (Pg. 2096)

DeCavalcante advised Lou Larasso⁵ that Carl Gambino³³ had removed Joe Bandy³⁶ (true Name Biondo) as Underboss, but that Joseph Zingaro³⁷ is still Caporegima. Gambino's cousin Pete Castellano³⁸ is another of his Caporegimes. (Newark Airtel to Washington dated 6/17/65) (Pgs. 2083-2098) (Pg. 2096)

B. On June 10, 1965, Joe Bayonne¹³ and Sam DeCavalcante discussed Bayonne's progress on being transferred from the Bonanno-DiGregorio Family to the DeCavalcante family.

DeCavalcante said he had discussed this with Carl Gambino who counselled against any move to transfer Zicarelli at this time, since Zicarelli is recognized as a "Producer", although he is only a soldier. (Newark Airtel to Washington dated 6/14/65) (Pgs. 2040, 2041)

C. Sam DeCavalcante told Sal Caternicchio³⁹ that Frank Majuri²⁶ is not only a member of the DeCavalcante family but is DeCavalcante's Underboss as well. (Newark Airtel to Washington dated 6/17/65) (Pgs. 2098-2100) (Pg. 2099)

6. That the Commission must approve new members.

A. On February 11, 1962, Angelo Bruno² in a discussion with Samuel DeCavalcante said, "Will you let me tell you something, Daylight⁴⁰ and Mike, these two fellows right before they were proposed, I went to New York because I still was not raised yet. We respect the Commission. Do you understand? And we couldn't do nothing without New York. I went to New York and said, "We are going to propose these fellows. There are people in the family who want to propose a few fellows, are we allowed to accept these proposals?" The Commission said, "Yes, you are allowed to accept them but only the administration has to know them." Nobody else, because the Commission said, "As soon as I propose anybody, everybody knows, including the law." They said the only ones, who have to know, is the administration in your family." Angelo Bruno went on, "Well they like me in New York. Let me tell you something. I know, before they made people, and Albert,⁴¹ poor guy, right? And another poor guy. I know this for a fact, they made them, and they didn't tell nobody, not even the families in New York."

Ignatius Denaro:³ "You're not suppose to, the Commission only does it if it is good." (Pgs. 74-75)

7. That members transfer from family to family.

A. On June 1, 1965, Samuel DeCavalcante met with his Underboss, Frank Majuri²⁶ and told Majuri that Joseph Zicarelli,¹³ also known as Joe Bayonne, was very desirous of switching from what was the Bonanno Family to the DeCavalcante Family. Zicarelli told DeCavalcante that his present family "uses" him too much. DeCavalcante advised Majuri that he had discussed this transfer with Carlo Gambino³³ but had heard nothing further from Gambino on this transfer. (Pg. 2011)

B. On June 11, 1965, DeCavalcante met with Louis Larasso,⁵ a Caporegima in his family. DeCavalcante claimed to Larasso that people from Carlo Gambino's family, people from Tommy Luchese's³² family, and people from Gasparino DiGregorio's⁹ family want to join the DeCavalcante family

because they know that DeCavalcante is a fair man and they have more chance to better themselves.

Larasso told DeCavalcante that Mooney³¹ was a lot like DeCavalcante. He said that Mooney stands up for his men like DeCavalcante and also like DeCavalcante allows his men to make money wherever they can. Larasso added that Mooney like DeCavalcante is also available to his men. Larasso said the Joe Venber, one of Mooney's men, told him that the family holds Mooney in very high regard as Mooney allows them to make money in any manner that they can. (Pg. 2218)

8. That members are ordered to murder.

A. On February 2, 1965, Samuel DeCavalcante had a discussion with his Underboss, Joseph LaSelva²⁹ about the problems of the Joseph Bonanno family.

DeCavalcante: "Bonanno⁸ put Magliocco³⁴ up to a lot of things like to kill Carl Gambino."

LaSelva: "Well Magliocco that was his son's father-in-law."

DeCavalcante: "Bonanno put Magliocco up to hit Carl Gambino³³ and Tommy Brown."³²

LaSelva: "Well that must have had something to do with Profaci's outfit?"

DeCavalcante: "Yeah, now they feel that Bonanno poisoned Magliocco. Magliocco didn't die a natural death. Because the only one who could accuse him of plotting against Gambino and Luchese was Magliocco. See Magliocco confessed to it. But Joe Bonanno did not know how far he went. Understand? So they suspect he used a pill on him, that Bonanno's noted for. So he knows the truth of all the damage he has done. But they feel he don't know how much the other people know. He'd come in and deny everything but he knows he could not deny he made people when the books were closed."

LaSelva: "Out on the coast there was some friction, wasn't there?"

DeCavalcante: "Well he tried to take California over, when they were having trouble. He sent the kid out there with forty guys. The Commission stopped him and that's where the trouble started. If he had listened to me, that time I went to him, this thing would have been straightened out. They would have just bawled him out."

LaSelva: "It's a shame. What was he, 58 or 59 years old, and the prestige that he had? What was he looking for? Anyway, it's really bad for the morale of Our Thing, you know? When they make the rules and then break them themselves. He's been in 20 years."

DeCavalcante: "Thirty-three years he's been in." (Pgs. 1273, 1274, 1275)

B. On February 23, 1963, Angelo Ray DeCarlo,⁴² Anthony "Tony Boy" Boiardo,⁴³ Samuel DeCavalcante, and Joe, possibly Joe Zicarelli were discussing how to kill a hood without embarrassing the victim's family. They said you don't want to shoot a guy so they give him a shot. (Pg. 99)

C. On February 23, 1963, Samuel DeCavalcante, Angelo Ray DeCarlo, also known as Gyp, Louis Larasso and Anthony Boiardo, also known as "Tony Boy", discussed the recent killing of "Cadillac Charlie"⁴⁴ in Youngstown, Ohio. All were critical of the method used and of the fact that his four year old son was also killed. DeCarlo stated that as a result of this murder the word had been passed that no hand grenades will be used in killing assignments in the future. DeCarlo further suggested that the best way to dispose of someone is to give the individual a fatal shot of dope and put him behind the wheel of his automobile where he will be found. (Newark Airtel to Washington dated 3/7/63) (Pgs. 111, 112)

D. On February 23, 1963, Anthony Boiardo,⁴³ also known as "Tony Boy", Samuel DeCavalcante, his Caporegima, Louis Larasso⁵ and Angelo Ray DeCarlo,⁴² also known as Gyp, discussed several murders.

Murder I

Tony Boy Boiardo: "How about the time we hit the little Jew."

DeCarlo: "As little as they are they struggle."

Boiardo: "The Boot⁴⁵ hit him with a hammer. The guy goes down and he comes up. So I got a crow bar this big, Ray. Eight shots in the head. What do you think he finally did to me? He spit at me and called me an obscene name."

DeCarlo: "They are fighting for their life."

Murder II

DeCavalcante: "Ray, you told me years ago about the guy where you said, 'Let me hit you clean'."

DeCarlo: "That's right. So the guy went for it. There was me, Zip and Johnny Russell. So we took the guy out in the woods and I said, 'Now listen' Zip had something on him. I said, 'Leave him alone Zip'. I said, 'Look', Itchie was the kid's name, I said, 'You got to go, why not let me hit you right in the heart and you won't feel a thing'. Itchie said, 'I'm innocent, Ray, but if you got to, do it', so I hit him in the heart and it went right through him."

Murder III

Further discussion of giving an individual a fatal shot of dope and putting him behind the wheel of his automobile where he will be found.

DeCarlo: "That's what they should have done with Willie Moretti.⁴⁶"

"You've got five guys here, you talk to the guy, tell him this is the lie detector stuff. You tell him, 'You say you didn't say this'."

Boiardo: "How many guys are you going to con?"

DeCarlo: "Well you don't con him then tell him. Now like you got four or five guys in the room. You know they are going to kill you. They say, 'Tony Boy wants to shoot you in the head and leave you in the street or would you rather take this, we put you behind your wheel, we don't have to embarrass your family or nothing,' that's what they should have done to Willie."

DeCavalcante: "They didn't want them on the street. They didn't want the rest of the mob to know that permission"

DeCarlo: "But I mean a guy like Willie Moretti. 'We like you and all but you got to go, you know it's an order, you gave enough orders'."

Boiardo: "I don't think Willie would have went for it."

DeCarlo: "I think he would, he would have tried to talk his way out of it but he would have went for it."

Boiardo: "It would have been better."

DeCarlo: "Sure, that man never should have been disgraced like that."

DeCavalcante: "It leaves a bad taste. We're out to protect people. When they made you they say an Italian phrase, 'don't not to abuse you, to protect people from being abused'; they made me in Italian, they all spoke in Italian." (Newark Airtel to Washington dated 3/7/63) (Pgs. 112, 113)

E. On June 16, 1965, Samuel DeCavalcante met with Tony last name unknown and another unnamed individual after the funeral of one Ciconia which took place someplace in the vicinity of Trenton, New Jersey and Bordentown, New Jersey.

Tony is believed to be a member of the family headed by Angelo Bruno of Philadelphia.

Tony related that once he had a job to do and he did it all by himself 30 years ago. He repeatedly mentioned the name Fillipo and he says that he and possibly two other individuals put Fillipo on a truck and tied him up. They drove him to a park, but the location was not satisfactory so they then put him in a car and drove him to a farm. Tony related that Fillipo was in the car and one of the others with him had turned up the car radio so that Fillipo's screams could not be heard. One of the subjects with Tony kept a gun to Fillipo's head. They took Fillipo to a farm and inside the garage on the farm, they cut Fillipo's throat. Tony described the conditions of the weather at this time as cold and he said that Fillipo's body was buried somewhere close to the

farm. For some unrelated reason, they decided to move Fillipo's body from the grave site so they went to dig him up. At this point Tony stated that he saw a sight that he had never seen before after they dug up the body and that he was scared. "We dug him up after he died, and his hair was still growing, the dead man was hairy, never saw this before." (New York Airtel to Washington dated 7/2/65) (pg. 2197)

F. Hit or murder of unknown individual by members of DeCavalcante family.

On April 16, 1965 through April 19, 1965 Samuel DeCavalcante had quiet whispered conversations with Louis Larasso,⁵ his Caporegima, and Bobby Basile,⁴⁷ his cousin and aide. Frank Cocchiaro,⁴⁸ Caporegima of DeCavalcante, and Ralph DeMeglio⁴⁹ were also involved. It appears that DeCavalcante and his associates eliminated someone although the victim's name is nowhere mentioned. It appears that Carl Gambino⁵³ was to be advised of whatever action was to be taken.

Previously on March 9, 1965, Louis Larasso had met with DeCavalcante. He had stated that he had heard that Carl Gambino, Joe Bandy,³⁶ Joe Zingaro,³⁷ Nick Melillo,⁵⁰ and Jimmy Failla⁵¹ were in partnership in the Mt. Vernon, New York garbage business. Included with them was one Joe Fiolo.⁵² DeCavalcante said he was aware of this and planned to ask Carl Gambino if he knows that Bandy, Zingaro, Failla are connected with the deal.

Larasso had advised DeCavalcante that Joe Fiolo has repeatedly telephoned him concerning another garbage deal. Fiolo has a brother or brother-in-law in the garbage business in New Jersey and wants Larasso to enter a partnership with this person. Fiolo has been contacting the Ford Motor Company in Metuchen, New Jersey and eventually expects to secure this stop for Larasso and Fiolo's relative. Fiolo expects Larasso in turn to locate a suitable dumping site. Larasso has been putting Fiolo off until he could consult with DeCavalcante. DeCavalcante told Larasso that he would see Gambino about Fiolo's proposition, in the meantime Larasso should continue to stall Fiolo diplomatically. DeCavalcante said he has heard that Fiolo is in trouble with Carl Gambino since he has been accused of stealing garbage customers from Joe Columbo.⁷

This information is set forth because it suggests that Fiolo may have angered Gambino sufficiently to cause Gambino to authorize Fiolo's elimination and that DeCavalcante had accommodated Gambino.

Information indicates that Fiolo is a member of a regime within the Gambino family, possibly that of Joe Zingaro. (Newark Airtel to Washington dated 4/21/65) (Pgs. 1702-1713)

9. That the Boss of a family is interested in machines to dispose of bodies.

A. On September 3, 1964, Samuel DeCavalcante had a discussion with two unknown males concerning various types of machines suitable for disposing of a body. One machine was mentioned as being capable of turning a body into a "meatball".

One of the unknown males said that the best machine was that which smashed up automobiles. DeCavalcante said he was looking for the type of machine which pulverizes garbage. The unknown stated that the only type that we know of that will pulverize garbage is a machine that Louie Larasso told the males about the other day and added "they are working on it now".

It appears that DeCavalcante wants the machine on hand in the event that he needs it. (Newark Radiogram to Washington dated 9/10/64) (Pg. 170)

10. That members of a family must follow Cosa Nostra protocol.

A. On February 23, 1963, Anthony Boiardo,⁴³ also known as Tony Boy, Samuel DeCavalcante and Louis Larasso,⁵ his Caporegima, met with Angelo Ray DeCarlo,⁴² also known as Gyp. Larasso announced that Andy "Ham" Dolasco⁵³ could not make it.

DeCarlo: "Andy Dolasco with his appointments. He's got to see his Caporegima, he's got an appointment. Everything by the book."

DeCarlo: "I need to get hold of a guy in Los Vegas and how the hell am I going to get hold of him? They don't even want you to make a call there."

Boiardo: "You can not call the state of Nevada. That's the orders." (Newark Airtel to Washington dated 3/7/63) (Pg. 109)

B. On September 22, 1964, Samuel DeCavalcante asked his Underboss Frank Majuri²⁶ if he could get in touch with Angelo Caruso²¹ and wondered if he could do business with Caruso that night. Majuri replied he would try to reach Caruso and ask him if he would meet with DeCavalcante late that evening.

Later on the same day DeCavalcante was advised by Frank Majuri that he had been in touch with a Dino through whom he had sent a message to Caporegima Angelo Caruso that DeCavalcante wanted to meet him. Majuri was advised later by Dino that Caruso had had orders not to meet with anyone. DeCavalcante regretted this, stating that in view of his long-standing friendship with Caruso he had hoped that Caruso would take a chance. (Newark Airtel to Washington dated 9/28/64) (Pg. 232)

C. On October 9, 1964, Frank Cocchiaro,⁴⁶ a Caporegima in the DeCavalcante family, met with DeCavalcante.

Cocchiaro: "We got an agent on the payroll."

DeCavalcante: "Who."

Cocchiaro: An agent on our payroll. The agent sent back word to our man that he heard that Sonny Franzese⁶ put up the money for the still. Now there's a stool pigeon right around Sonny Franzese's. Now, if it ever got back to the agent's office that this was said there would be a big stink over it. I must get to Sonny Franzese so that he don't just turn around and say 'how do you like that, the agents know that I put up the money for this thing'. The guy right next to him might be the stool pigeon that the agents got it from, 'how can I do this?'"

DeCavalcante: "We will tell Joe Columbo⁷ and hold Joe Columbo responsible. I am going to have an appointment with Joe if you want to come in." (Newark Airtel to Washington dated 10/20/64) Pgs. 335, 336)

D. On June 11, 1965, DeCavalcante met with Louis Laraso,³ his Caporegima. DeCavalcante told Laraso that he had sent Joseph LaSelva,²⁹ an Underboss of DeCavalcante, to Joseph Sferra,²⁷ also known as Joe Tiger, to notify Sferra of his demotion from Caporegima to soldier and the reasons for the demotion. DeCavalcante had also told LaSelva to tell Sferra that he was not the delegate for the hod carriers Local number 394 any longer. LaSelva only told Sferra he was no longer a Caporegima and nothing else.

DeCavalcante related that on June 10, 1965, Sferra met him and Sferra apologized for not having done his duty as a Caporegima and apparently did not know that he was not the delegate for Local number 394 any longer. DeCavalcante had to tell Sferra that he was no longer the delegate which reduced Sferra to tears. DeCavalcante said, "Sferra kept saying 'this is awful' after being told the foregoing. DeCavalcante categorically pointed out to Sferra why DeCavalcante had removed him from both positions. DeCavalcante told Sferra that he forced DeCavalcante into doing these actions even though DeCavalcante did and still does like Sferra personally. DeCavalcante said "Our People" had to be given preference over their personal friendship and Sferra was removed for the good of the DeCavalcante family. DeCavalcante further pointed out to Sferra that if he did not take these actions, in time, the other DeCavalcante members would feel that DeCavalcante and Sferra were in league together and would think that DeCavalcante was as bad as former Bosses, such as Phil Amari.¹¹³

Laraso suggested Sferra had been punished enough with being removed as delegate and Caporegima. (Pg. 2215)

11. That the Boss of the family approves destruction of a debtor's building by arson in order to collect the insurance and pay the shylock loan but "does not want to know".

A. On June 3, 1965, Samuel DeCavalcante was discussing with Bobby Basile,⁴⁷ his cousin and a member of his family, some

of the shylock money owed to DeCavalcante. The following discussion resulted.

Basile: "Mr. Maglie⁵⁴ wants to burn down his joint and I got the guy."

DeCavalcante: "Who's the guy?"

Basile: "Russ; as far as Pussy's concerned he says 'O.K.' It's up to you now."

DeCavalcante: "What's he want to pay for it?"

Basile: "He's going to pay \$5,000.00, that's all. I'll give him a break, he's got \$90,000.00 insurance on it."

DeCavalcante: "I don't need to know nothing."

Basile: "O.K. done, O.K.?"

DeCavalcante: "How's he going to pay you when he collects the money or what?"

Basile: "He's going give one thousand. I let the kid make the arrangements. I didn't step in, I just introduced them so he's going to give the kid a thousand to get the stuff, you know."

DeCavalcante: "I don't want to know nothing about it."

Basile: "You don't want to know so I told Pussy⁵⁵ and he said, 'Well I don't care'. I said, 'Look and I didn't tell you nothing? You want to leave it that way?' 'Yeah' Pussy said, 'I don't care'."

DeCavalcante: "Forget about it."

Basile: "Okay, I didn't tell Pussy I spoke to you or nothing so it's forgotten." (Newark Airtel to New York dated 7/15/65) (Pgs. 2105, 2106)

12. That the Boss has Political Contacts who are friendly and do favors for the Boss and for the family.

A. On May 25, 1965, DeCavalcante met with Dave Margolis. In a boast, DeCavalcante claimed that he has done favors for a person in the office of Governor Hughes of New Jersey. DeCavalcante said that, in return, he receives information from this person about what this person learns concerning the interest of law enforcement agencies in DeCavalcante.

Margolis told DeCavalcante that he has a liquor-delicatessen type store in Newark, New Jersey from which he sells bottles of liquor on Sunday which is against the law. Margolis was caught doing this and DeCavalcante and he met with a New Jersey Alcohol Beverage Control official on May 24, 1965 and DeCavalcante straightened out the trouble that Margolis had with the Alcohol Beverage Control in the state of New Jersey. (Pg. 2014)

B. On March 15, 1965, Sam DeCavalcante met with Emanuel Riggi,⁶⁶ father of John Riggi,²⁵ Caporegima in the DeCavalcante family. Riggi told DeCavalcante that he had received another letter from his attorney, concerning his pending deportation matter. DeCavalcante read the letter. Larry Wolfson,⁵⁸ a partner of DeCavalcante entered and mentioned that he had a luncheon appointment with Chris Franzblau,⁵⁶ attorney for DeCavalcante and Wolfson.

Riggi stated that his wife and his sister had been to see Congresswoman Florence Dwyer of the sixth congressional district in New Jersey and Mrs. Dwyer assured them that Manny Riggi would not be deported, even if he were found guilty of the charges, he is or will be indicted on. Mrs. Dwyer said however that Riggi must maintain a clean record in the future. (Pg. 1578)

C. On December 30, 1964 Sam DeCavalcante introduced Manny Riggi to an unknown person and advised this person that the Immigration and Naturalization Service is trying to deport Manny Riggi. DeCavalcante said that he had Chris Franzblau⁵⁶ working on it, looking at Riggi's Federal record. In discussing Riggi's troubles with the Immigration and Naturalization Service this person stated that he used to be close to Senator Williams of New Jersey. (Pg. 910)

D. On September 9, 1964, Bobby Basile, Bernie Furst,³⁷ Sam DeCavalcante and Larry Wolfson⁵⁸ were having a discussion of the business situation at Controlled Temperature, a company that is being run by Furst, Basile and Frank Cocchiaro but is actually financed by DeCavalcante.

Bobby Basile stated that he has a guy in Washington, D.C. who is trying to get United States Government money for Con-

trolled Temperature Company in Government contracts. (Pg. 376)

E. On October 14, 1964, Bobby Basile told Sam DeCavalcante that he expects a Small Business Administration loan. (Pg. 456)

On October 22, 1964 Sam DeCavalcante warned Bobby Basile in no uncertain terms that Basile is never to make a move without consulting Sam first regardless of what amico nos it is or how close the person may be to Sam DeCavalcante. DeCavalcante wants Bobby Basile to clear with him first. DeCavalcante referred to Basile's attempts to get a Small Business Administration loan DeCavalcante pointed out that Bobby Basile had no right to make decisions like this himself and must never do it again. The loan was to be negotiated by Danny Noto⁵⁹ through some friends that he has in the Small Business Administration. DeCavalcante noted that Danny Noto is sometimes irrational, citing his current dislike for Whitey Joseph Danzo⁶⁰ who Noto suspects of stealing from him. (Pg. 554)

F. On October 20, 1964, Sam DeCavalcante and Joe Kremer⁶¹ were discussing the case of Nick Quarino,⁶² a Cosa Nostra member, who had just been sentenced to imprisonment for one to two years. DeCavalcante mentioned that he had talked with Kinnealy⁶³ and that he had told Sam the same thing that the Republican had told him, namely that someone had been looking for the Prosecutor's job in Union County. Sam mentioned that Collandra is not an intelligent man but has connections; he is a connection man. Sam mentioned that in talking with Kinnealy there were political angles concerning this case and that Quarino was a victim of politics at this time of the year, namely just before elections. (Pgs. 482, 483)

G. On June 14, 1965 Sam DeCavalcante and his Underboss, Frank Majuri⁶⁴ were discussing a Judge Ard⁶⁴ of Elizabeth, New Jersey. DeCavalcante said that Sam Reida⁶⁵ is having a zoning problem in Clark Township, New Jersey and the decision will rest with Judge Ard as to whether Reida can build what he wants. (Pg. 2147)

H. On June 23, 1965, Samuel DeCavalcante had a discussion with his partner Larry Wolfson⁶⁶ about the fact that the Union County Democratic Party leader had sent Marabelli from Elizabeth to see him.

DeCavalcante was told by Marabelli that the Union County Democratic leader had learned that DeCavalcante had been contacting various people in an effort to assist Sam Reida.⁶⁵ Reida was desirous of building numerous garden apartment buildings on land that he owned in Union County. This land was in an area which was zoned for this type of building. The residents in the immediate area of this planned construction site had brought Reida to Court in an effort to keep him from constructing garden apartments

All the arguments had been entered by both sides and Judge Ard had the suit under consideration. Marabelli told DeCavalcante that the Democratic Leader controls Judge Ard and that the Judge would give Reida a favorable decision if he was told to do so by the Democratic Leader

DeCavalcante told Wolfson that Reida would have to pay the Union County Democratic Leader "a couple of thousand" if Reida wants the leader to tell Judge Ard what decision to give.

Wolfson told DeCavalcante that he had met with Reida on June 23, 1965 and that Reida had told him that he was confident that the Judge would find for Reida on the basis of Reida's lawyer's arguments on behalf of Reida's right to construct garden apartments on the land

DeCavalcante told Wolfson that he does not trust nor like Marabelli and suggested that Marabelli may have arranged a shakedown in this matter with the Union County Democratic Leader and/or Judge Ard.

DeCavalcante told Wolfson to telephonically contact Reida from Ange and Mim's and advise him of this latest development (Pgs. 2187, 2188)

I. On January 23, 1965, Emanuel Riggi⁶⁶ met DeCavalcante at DeCavalcante's request.

DeCavalcante was very concerned about three young New Yorkers who were in trouble with the Elizabeth, New Jersey Police Department. Riggi was detailed to contact Gus Brugger,⁶⁷ who had recently been appointed the Police Director of Elizabeth.

The following conversation ensued:

DeCavalcante: "One of these kids is on probation. They cannot be fined. It has to be thrown out and this guy has to do his best to throw this out. This is personal! And I'll see that they don't even come in Elizabeth anymore. That I'll guarantee."

Riggi: "If I'd known about this probation—because his exact words—he told me they were going to throw the book at him because he's hot. They're from New York. Are they from New York?"

Riggi: "They're from New York. He said, 'I don't want no punks around here;' in other words, he was trying to tell me he wants the town clean for a while."

DeCavalcante: "Tell him, 'Sam will keep the town clean for you, these guys won't even come in.'"

DeCavalcante: "Manny, go back tonight! I'll ask these kids to get their lawyer to postpone it. Then we'll have it thrown out—this has to be thrown out because this kid's in trouble and a thing like that—he could be put away for a long time."

Riggi: "Well he wants the town clean because he's just starting."

DeCavalcante: "Tell him I'll guarantee him nobody wants the town cleaner than us. And tell him there's a gift in it for him."

Later the same day DeCavalcante told his Underboss, Frank Majuri:⁶⁸ "Tell them over there they got nothing on these kids. Don't try to make any connection because we are working on the case—don't panic." (Pgs. 1097, 1098, 1099)

J. On February 3, 1965, DeCavalcante met with Joseph Arthur Zicarelli,¹³ also known as Joe Bayonne. They discussed the three young New Yorkers who were arrested in Elizabeth on January 14, 1965, and charged with suspicion of burglary. Zicarelli had requested DeCavalcante to use his influence to have the charges dismissed. The following conversation ensued.

DeCavalcante: "Those three guys—after I spoke to you they showed up and they were thrown out."

Joe Bayonne: "Yeah, I know. I tried to get you back and couldn't."

DeCavalcante: "Well what happened to them? These guys are nuts."

Joe Bayonne: "They were there! he called right away and they said they were dismissed so they left."

DeCavalcante: "You know when I called you, it was in the afternoon. I even called this guy back because he called the clerk and told the clerk to postpone it for a week. They were there at 11:30 instead of 9:30."

Joe Bayonne: "What do we have to give this guy?"

DeCavalcante: "Nothing. Forget about it."

Joe Bayonne: "Why should I forget about it? These weren't three of my guys. They want to pay. Let them pay. What did you give the guy?"

DeCavalcante: "I'm suppose to see him next week. Joe, if it's you . . ."

Joe Bayonne: "It's not me! I don't know these kids, Sam."

DeCavalcante: "Well you sent them down."

Joe Bayonne: "You know Frankie Dee. These kids belong to Frankie and Nike. Let them pay. Why should you pay anything?"

DeCavalcante: "Over here I'm suppose to see the Judge and the Police Commissioner."

Joe Bayonne: "Alright—whatever you go for let me know."

DeCavalcante: "No. They're not your guys? Well let them go. I thought it was your guys. You asked for the favor."

Joe Bayonne: "Sure, they're the same as I am. It's Mike and Frankie Dee. And these kids are around them. Mike came in to see?"

DeCavalcante: "Now, with one understanding, these kids are never supposed to come around Elizabeth."

Joe Bayonne: "They know that."

DeCavalcante: "And they're not suppose to sue for false arrest. I guarantied that myself. I know they wouldn't do that anyhow."

Joe Bayonne: "They are good kids. They done plenty of work and they're around anytime you want them." (Pgs. 1276, 1277)

K. On April 7, 1965, Frank Majuri,⁵⁶ Underboss of DeCavalcante, met with Chris Franzblau,⁵⁶ attorney for DeCavalcante. He briefed Franzblau on an incident in Elizabeth, New Jersey which resulted in the arrest of his son, Charlie Majuri.⁷⁰ According to Frank Majuri, Charlie was living with a girl and under the guise of a bookmaking raid, police broke in and arrested them and then seized pads, papers, pencils and so forth as "evidence". The hearing for Charlie Majuri was set for April 10, 1965.

Franzblau claimed to be very friendly with the Union County Prosecutor, Leo Kaplowitz⁷¹ and said he would see what he could do.

Majuri stated that this action against his son was really just harassment, directed at him, because he and Louis Larasso⁵ were caught at Appalachin, New York, November 1957.

Franzblau advised that the only safe procedure before a Grand Jury was to claim protection of the fifth amendment to every question, no matter how innocent. (Pg. 1676)

On April 12, 1965, Louis Larasso contacted Sam DeCavalcante and they discussed the Charlie Majuri arrest. DeCavalcante said that Union County Prosecutor Leo Kaplowitz thought that there should have been a motion to suppress the evidence. Kaplowitz suggested that a lawyer named Isaacs should be retained.

Larasso suggested an offer be made in this matter and said that he would be willing to see the thing settled for three thousand dollars, even if it was a shakedown, rather than to see the thing go to the County level, where there might be pressure from the F.B.I. to prosecute.

DeCavalcante indicated a willingness to spend one thousand dollars—five hundred dollars to the Judge and five hundred dollars to Elizabeth Mayor Tom Dunn⁷²—providing the matter could be handled in Court. (Pgs. 1729, 1730)

L. On October 12, 1964, Sam DeCavalcante and Joseph "Whitey" Danzo⁶⁰ were discussing a gambling raid that had taken place in Elizabeth, New Jersey over the weekend and the paper had made a big thing of the raid stating that it was a distribution center for twin doubles and gambling activities.

Danzo mentioned that he had talked with Thomas Dunn,⁷² who was running for Mayor of Elizabeth on the Democratic ticket. Danzo stated that they would pull good with the new administration, if they got in. He also said that a Bunchy Grant had made a big contribution to the campaign.

Danzo then mentioned that Mayor Steve Bercik,⁷³ who had been Mayor of Elizabeth for eight years, hated Louis but that Bercik would not get the Prosecutor's job or anything. He said that Bunchy Grant knows the ins and outs of the whole setup in Elizabeth. (Pgs. 448, 449)

On October 23, 1964, Thomas Dunn⁷² of Elizabeth, New Jersey, candidate for Mayor of that city, visited Sam DeCavalcante and was introduced by Sam to Larry Wolfson,⁵⁸ DeCavalcante's partner.

The following conversation ensued.

DeCavalcante: "After November 3, you address him as Mayor."

Dunn: "We hope."

Dunn: "I been waiting for it for fifteen years."

DeCavalcante: "Do you think we could get any city work?"

Dunn: [Laughingly.] "Well maybe."

Dunn related some of the trials and tribulations of his campaign and he addressed DeCavalcante as "Sammy".

Dunn said: "I'm worried about one area—the third ward—a big Jewish area."

DeCavalcante offered unlimited assistance to Dunn, noting that he planned to be away for the next week and suggested that his "Paisons" would handle anything for him.

Dunn said that at a debate the previous night he was charged with being connected with gambling interests in Elizabeth.

Dunn: "If you have any way of getting to Magnolia⁷⁴ and LaCorte⁷⁵ tell them to keep their lousy mouths shut because you know better than I do that I have no"

DeCavalcante: "Oh, sure."

Dunn: "Because this thing could cream me at the last minute. So, if you can in some way get to these two guys, tell them to keep this thing out of the papers."

DeCavalcante: "It's a lot of talk. He couldn't come out with a thing like that with no proof."

Dunn: "Well, just by association, Sam. So if you have any way of getting to Magnolia."

DeCavalcante: "I sure will."

DeCavalcante pledged his support to Dunn and guaranteed him that in their future relationships no one from Sam's organization will ever be the cause of any embarrassment to Dunn.

Dunn: "That's good enough for me."

DeCavalcante: "So I wish you a lot of luck. Can you use this in your campaign?"

Dunn: "Thank you, Sam. You bet I can use it. Enjoy your trip to Florida. When are you leaving?" (Pgs. 603, 604)

On November 5, 1964, Louis Larasso⁵ advised Sam DeCavalcante that Thomas Dunn⁷² had won the Mayoralty election in Elizabeth, New Jersey by 9,000 votes; they then discussed Larasso's payments. (Pg. 563)

M. On November 24, 1964, Sam DeCavalcante mentioned to Louis Larasso⁵ that he had received a phone call from the guy that went to see the Judge—not the Senator but the Judge—about Mickey Quarino.⁶² This fellow wanted to see DeCavalcante. DeCavalcante said he was looking for something. So he told Frank Majuri⁶⁶ that he would give three hundred dollars. He asked if that was all right with Larasso. Larasso indicated that it was all right. Then DeCavalcante said that this was not taking care of the Senator. Joe Zicarelli¹³ had said forget about it. (Pg. 793)

N. On September 8, 1964, Sam DeCavalcante introduced Phil Camoro⁷⁶ to Louis Larasso as his cousin. He told Larasso that Camoro was "married" to Anthony "Little Pussy" Russo.⁷⁷

DeCavalcante said that Russo had eighteen thousand dollars invested in a deal in Florida but had taken eleven thousand dollars out, leaving a balance of his investment at \$7,000.00. DeCavalcante said that he would offer \$3,500.00 to Russo for half of the Florida deal. If Russo accepts his offer, DeCavalcante will make Camoro a full partner with Russo.

Camoro stated that he has been the State of New Jersey Commissioner of Tenement Housing for nine years, having originally been appointed by Governor Robert Meyner, and still has a couple of more years to serve under Governor Richard Hughes. (Newark Radiogram to Washington dated 9-16-64) (Pg. 172)

While with Sam DeCavalcante Phil Camoro placed a call to Tishman Realty Corp. at 666 Fifth Ave., New York City, and asked for Mr. Leonetti [phonetic]. Phil Camoro referred to himself as Commissioner Camoro and explained that he might soon be tied in with an oil concern and would be interested in servicing Tishman's two thirty-story buildings in Fort Lee, New Jersey. (Pg. 144)

O. On February 23, 1963, Anthony Boiardo,⁴³ also known as Tony Boy, Sam DeCavalcante and his Caporegima, Louis Larasso³ met with Angelo Ray DeCarlo,⁴² also known as Gyp.

Among the many things that were discussed were the following:

Boiardo: "I don't want to see Tony Bananas⁷⁸ anymore. I told Louis 'You go back and tell Bananas that 'Ham' Dolasco⁸³ has got a beef. That Dolasco still wants a piece of the Monte game like it was originally set up'."

DeCarlo: "Is Tony Bananas still going with the Monte Game yet?"

Boiardo: "No, Dick Spina⁷⁹ told him to stop."

Boiardo: "You know Dick Spina asked me, 'Why don't you and Ray DeCarlo get together and open up?' I said, 'What is there to open up?'"

Boiardo: "You know Hughie Addonizio got hold of me, he said, 'Look, tell Ray DeCarlo that the F.B.I. knows about Irving Berlin.'⁸¹ I'll tell you how much the F.B.I. knows" (Newark Airtel to Washington dated 3-7-63) (Pgs. 109, 110, 111)

P. On February 5, 1965, Joseph Arthur Zicarelli¹³ visited Samuel DeCavalcante. When he arrived Emanuel Riggi⁶⁶ and his son, John²⁵ were also present. DeCavalcante introduced them to Zicarelli as "amico nos" although Zicarelli recalled that he had met Emanuel Riggi once before.

Emanuel Riggi had been in the process of telling DeCavalcante of the progress of his deportation case. He mentioned that an Olivetti, who was formerly with a U.S. Government Agency, had advised him to contact Representative Florence Dwyer of New Jersey and Senator Harrison Williams of New Jersey in an effort to interest them in the case. Olivetti told Riggi that he had his permission to use his name.

Zicarelli was aware of Riggi's troubles having heard of them previously from DeCavalcante. In fact, he was able to report that at DeCavalcante's request, he had spoken in behalf of Riggi to his friend the Congressman, Cornelius Gallagher, of New Jersey. Zicarelli said that he has not heard from his friend since because of "all the commotion". This may have referred to the Federal Grand Jury hearings in the Southern District of New York. Zicarelli indicated that he would follow up this matter and said that he was sure that Gallagher could help if all else failed.

Emanuel Riggi mentioned that his lawyer is Chris Franzblau⁹⁶ who was a former Assistant United States Attorney. Zicarelli cautioned against trusting Franzblau too far, citing an instance where as an Assistant U.S. Attorney, he attempted to send Zicarelli's wife to jail. DeCavalcante vouched for Franzblau's trustworthiness.

DeCavalcante said: "Nick Delmore¹ trusted Franzblau all the way. Nick put him in his office there and with me, he's always been respectable. He's done what I told him to do."

Zicarelli acknowledged that Franzblau is pretty close with this Satz⁹² guy and this connection might be useful. (Newark Memorandum to Washington dated 2-10-65) (Pgs. 1185, 1186)

13. That the Boss and Family members had contacts with law enforcement people at all levels who could and did do favors for the Boss and his Family.

A. On February 23, 1965, Corky⁸³ met with Sam DeCavalcante. Corky told Sam about a crap game that Joe Columbo was opening in Staten Island, New York. He said that Joe Columbo asked him to go see a certain lieutenant in the Staten Island Division of the New York City Police Department and that it was finally agreed that the Police Department was to be paid \$2,850.00 a month. The only stipulation was that no cars were to come from New York, namely Manhattan, Brooklyn, but that the people in Staten Island were to go in cars and pick up the people in New York and bring them to the game. (Pg. 1263)

B. On February 1, 1965, Sam DeCavalcante was visited by one Mickey and they discussed recent numbers losses that they both had suffered. Mickey was paid an undetermined amount of money by Sam and thanked him for it.

DeCavalcante and Mickey then discussed a crap game which was in the process of being set up by Mickey. Mickey told Sam that he had an "okay" from Chief John Ellmyer, Jr.⁸⁴ of Edison Township but needed a contact on the county level which was to have been made three weeks ago by Dutch Mele

They discussed crap games in general and Sam pointed out that in order to make money it is necessary to have many players betting both ways, so that on each roll, the house gets its steady 5%.

Mickey mentioned that he had been referred to Pangy, (true name D. Raimo), as one who could bring affluent players to his game. He was aware that Pangy is Ray DeCarlo's⁴² man but that DeCarlo is not now operating. Sam said that he has known Pangy for years, describing him as a "big guy" and a "creep". DeCavalcante said that Pangy charges \$35.00 per car to bring players in, but that the players are all hustlers and it is not worth it. DeCavalcante recalled that he once had a small game and could not make any money even though he employed a "bust-out man".⁸⁵ (Pg. 1206)

C. On December 30, 1964, Sam DeCavalcante met with Emanuel Riggi.⁶⁶ DeCavalcante told Riggi that he had heard that the Union County Prosecutor⁷¹ was giving George Malgeri, proprietor of Lu-Mal Club on U.S. Highway 1, Elizabeth, New Jersey, a real headache. The Prosecutor wants to charge Malgeri with manslaughter.

Riggi told DeCavalcante that he and his son, John Riggi²⁵ would probably see the Prosecutor that evening. Riggi wondered about the contents of the police reports submitted by Captain Brugger,⁶⁷ who is to be the newly appointed Police Commissioner of Elizabeth.

DeCavalcante suggested to Riggi that he tell the Prosecutor that they were well acquainted with "Pickles", whose true name was Angelo Piccoellole,⁸⁶ who had died as a result of a beating, and that they knew him to get drunk and to become nasty. They have no doubt that "Pickles" started the fight which resulted in his death, but the whole thing was an accident.

Riggi attempted to contact Captain Brugger telephonically but learned that he was at a meeting with Mayor Thomas Dunn⁷² of Elizabeth.

Later, Frank Majuri²⁶ visited DeCavalcante. They discussed the possibility of an indictment against George Malgeri. Elizabeth Police Department had turned in a favorable report regarding the "Pickles" incident and maintained that Malgeri could not be charged. He also offered to testify on Malgeri's behalf. DeCavalcante therefore concludes that the efforts of the Prosecutor of Union County⁷¹ were designed to accomplish a shakedown.

Majuri told DeCavalcante that he had heard that Malgeri is scheduled to appear before the Grand Jury in Union County on January 4, 1965, and that the Prosecutor will seek an indictment.

DeCavalcante described the Prosecutor, Leo Kaplowitz,⁷¹ as a stupid kid. He said that another officer, possibly Al Goegelman, was trying to make a case against Malgeri. Goegelman was the head of the Vice Squad of Elizabeth Police Department at the time. DeCavalcante told Majuri to tell Malgeri that he has nothing to worry about. DeCavalcante added that he would like to give Brugger something.

Majuri told DeCavalcante that he had given Brugger some whiskey and \$100.00 for Christmas. DeCavalcante told Majuri to take him other presents. (Pgs. 953 a-c)

D. On December 30, 1964, Emanuel Riggi⁶⁶ reminded DeCavalcante of having spoken of a Pete Smith⁷⁷ in Trenton, New Jersey. Riggi said that Smith is now head of the Fraud in Newark and covers the entire State of New Jersey.

Riggi said that he had met with Smith the previous day and that Smith can get "anybody's record." Riggi produced what was probably his own F.B.I. identification record noting that Smith had removed certain identifying marks which would show that it had come from him.

Riggi said that his arrests which occurred in the early 1930's were mostly unimportant except for one which took place in Jersey City.

Riggi told DeCavalcante that Pete Smith had advised him to get a good lawyer, suggesting Grover Richman⁸⁸ or Angelo Malandra⁸⁹ and Smith offered to lend Riggi \$500.00 to defray legal expenses.

Riggi added that Smith also gave him a record for one Joseph Sferra⁸⁷ on which was shown an arrest for receiving stolen property. Smith warned Riggi that Sferra should have this old charge expunged. Riggi and DeCavalcante decided that this record did not apply to the Joseph Sferra that they knew, due to discrepancies in date and place of birth. (Pg. 953-b)

E. On January 18, 1965, DeCavalcante was visited by Bobby Basile⁴⁷ and Joseph "Whitey" Danzo.⁶⁰ DeCavalcante related that Mickey had been in to see him about opening up a crap game. "Whitey" Danzo said that he had argued with Mickey who wanted to open without telling Sam DeCavalcante.

"Whitey" Danzo tried to tell Sam DeCavalcante about his differences with Mickey. He indicated that Dutch Mele was trying to help Mickey get started and said that he had Joe Kelly,⁹¹ the New Jersey State Trooper, on the pad. Danzo would not give them any satisfaction, so Dutch Mele went directly to "the Count", Emilio DeLeo true name. "The Count" then called "Whitey" Danzo for an explanation and Danzo then had to censure Dutch Mele for this interference. Sam DeCavalcante ordered "Whitey" Danzo to tell Mickey to stay away from Dutch Mele.

Danzo then related that he had been warned by possibly Dutch, who was friendly with the Chief John O'Malley,⁹⁰ that the F.B.I. had been taking license numbers and pictures around a store in South Plainfield where there was a numbers operation. "Whitey" Danzo had been warned that the F.B.I. is interested in him, but according to him, the F.B.I. has him confused with another Whitey. (Pgs. 1066, 1067).

F. On February 23, 1963, Angelo Ray DeCarlo⁴⁷ was visited by Anthony Boiardo,⁴³ also known as Tony Boy, Sam DeCavalcante, and Louis Larasso,⁵ his Caporegima.

Boiardo was discussing the \$5,000.00 that each of the Leaders had put up for payoff in Newark.

Boiardo: "Yeah, Ham Dolasco⁵³ wanted me to tell his Caporegima that we all put up the \$5,000.00 in Newark and that Tony Bananas⁷⁸ did not keep his word."

DeCavalcante: "You know Tony thirty or thirty-five years ago if an—was ever seen talking to a cop they looked to hit him the next day. They figured he must be doing business with the cop."

DeCarlo: "Today, if you don't meet them and pay them you can't operate."

Boiardo: "The only guy I handle is Dick Spina.⁷⁹ Gino Farina⁹² and them guys handle the rest of the law. About seven or eight years ago I used to handle them all."

DeCavalcante: "Did you ever see the way 'Ham' Dolasco operates on 14th Street?"

DeCarlo: "For \$5,000.00, 'Ham' Dolasco and Tony Bananas thought they bought a license."

DeCavalcante: "This was before the \$5,000.00."

DeCarlo: "They walk into precincts and everything. You can't have a man and be seen with him. He's no good to you then."

DeCavalcante: "And how long do you think it will take the Federal men to find out." (Pg. 110)

G. On September 14, 1964, Samuel DeCavalcante was visited by Anthony Perry Santoli,⁹³ also known as Jack Panels, a Lieutenant of Angelo Ray DeCarlo.⁴² Jack Panels told DeCavalcante that he will open a crap game on Wednesday or by Friday, at the latest, in New York.

Panels said that he has a "solid okay" with the Division and the Borough Police of the New York City Police Department. Panels borrowed \$5,000.00 from DeCavalcante and will have to put up a total of \$12,500.00 to run the game in which he will have a one-third interest.

Panels told DeCavalcante that he has been on his own for a while but that he has never lost any money in New York and

that this will be a bigger game and he should get a bigger piece of the action. He indicated that he would need the money for about ten or twelve days and would have it back to DeCavalcante in two weeks at the latest. (Newark Radiogram to Washington dated 9-15-64) (Pgs. 191-197)

H. On November 23, 1964, Larry Wolfson,⁵⁸ partner of DeCavalcante, told Sam DeCavalcante that he had been arrested for a traffic violation the previous Saturday by the New Jersey State Police but that Sisco took care of it. He said the arresting officer was Sinsky "from the shore" but Wolfson had Sinsky call Sisco who was assigned to the Bloomfield, New Jersey barracks of the New Jersey State Police.

DeCavalcante said that he was giving a case of liquor, in pints, to the Bloomfield Barracks where Sisco is stationed and a half of case for the New Jersey State Troopers on the Garden State Parkway. DeCavalcante suggested that Larry Wolfson give the other half of the case to the "shore barracks" of the New Jersey State Police. Wolfson objected mildly to this suggestion of gifts. However, DeCavalcante indicated to Wolfson that he would get him a "courtesy card for the Parkway." (Pg. 761)

On December 7, 1964, Larry Wolfson⁵⁸ told Harriet Gold,⁹⁴ his sister, who is the secretary of DeCavalcante, that he has a bill for two cases of Scotch for the Police. (Pg. 736)

I. On October 23, 1964, Samuel DeCavalcante was told the following by Joseph "Whitey" Danzo:⁶⁰ "Now after the election—this guy⁹⁵ that we had before, that got this big job with the United States Security—the guy, we had with the County, sent a message to me. They offered him everything over here if he comes back, fifteen thousand a year salary and everything. After election, he can come back if he wants to. The only way he'll come back is, if we work with him. He don't want to come work with anybody else. But, he wants to know that there's something to come back to—where he can make some money. Otherwise he ain't coming back, he's still in the Department. Now he'd promise but never fill the promises."

DeCavalcante: "Dese louse guys."

Danzo: "But he pulls good with all them outfits—the other law enforcement agencies—this guy. He knows all the moves they make. He told me now that the State is around the area, hot and heavy. He said they are around Plainfield and the New Brunswick area. He said, 'Take it for what it's worth'. He's supposed to be waiting for Saigon, you know. He told the Police Force—'How about Dan,⁹⁵ for the Mayor',—you know." (Newark Airtel to Washington dated 11/9/64) (Pgs. 575, 576, 601)

J. On September 14, 1964, Jack Panels⁹³ asked Sam DeCavalcante if he had anything going in Essex County.

Sam replied, "No." The following conversation ensued:

Panels: "Unless you got a real good friend—we don't like to kick this around—because if it leaks out—these guys will come the following week and really catch everybody. But, if you got any good friends, the Feds⁹⁶ are going in there this week."

DeCavalcante: "Essex?"

Panels: "Yeah."

DeCavalcante: "Did you tell Jerry?"¹²

Panels: "Yeah, they told us two weeks ago they were going into Monmouth County and they hit Monmouth County."

DeCavalcante: "How come Pussy⁷⁷ got closed?"

Panels: "Cause he likes to hide things. He's got a million connections. I was there last week."

Panels emphasized that he will always accept a tip of this sort gratefully.

Panels: "Anyway, they're definitely coming in next week—the Feds—looking for stamps—bookmaking, horses or numbers. But getting back to this thing" (Pgs. 242, 243)

K. On February 26, 1965, Sam DeCavalcante told Frank Majuri,⁹⁸ his Underboss, Lou Larasso,⁵ his Caporegima, and two other individuals that the group should be very careful the coming week-end. He said that the New Jersey State Police were

going to move in certain areas and that he will find out more later from Joe Bayonne.¹³ DeCavalcante mentioned specifically Union County and he told the group to warn everyone to be careful not to be caught in any raids. (Pg. 1312)

L. On September 3, 1964, Samuel DeCavalcante was contacted by an unidentified male who is affiliated with a Construction Trades Union. This person told DeCavalcante that he had received a warning concerning a sports and numbers parlour in which the law enforcement authorities were interested. He said that the Internal Revenue Service, Detective Clinton Pagano of the New Jersey State Police and "the Prosecutor's" men were aware of two telephone numbers with prefix UN from which betting was being handled. This person further stated that he had called "Mike from Old Bridge" who was vacationing in the Poconos and told him not to come home, because the authorities were waiting for him to appear at the Sports Palace before raiding the place. This person further told DeCavalcante that his only interest in the matter was in discharging his responsibility by advising the persons running the operation. DeCavalcante and this unidentified caller decided that they would notify Angelo Ray DeCarlo, who they believed had control of the parlour. (Pg. 214)

M. On March 19, 1965, Corky,⁸³ met with Sam DeCavalcante. He told Sam that he had been arrested and was out on \$10,000.00 bail. He said that he had been charged with the crimes burglary, grand larceny and coercion by the New York City Police Department. He emphasized that the police have tapes involving Rocky,⁸⁷ Micky Dee,⁸⁹ Frank,⁴⁸ and everybody and that they had let Corky listen to the tapes for two hours.

Corky advised that he was carrying on his person receipts pertaining to an illegal still. Once in the 102nd Police Station of the New York City Police Department located in The Borough of Queens, under the guise of being ill, Corky was able to dispose of the papers in a toilet.

Corky said that the interviewing officers attempted to convince him that Mickey Dee, Rocky, and Frankie were becoming annoyed at his repeated demands for money and were considering eliminating him. To emphasize their point, they allowed Corky to hear tape recordings of telephone conversations between Mickey Dee and Rocky, who was then in Hot Springs. Corky said he wanted to advise Sam DeCavalcante that if he suspected any foul play against himself, he intended to act quickly to protect himself.

Sam assured Corky that he would let it be known that, if any harm came to him, both Mickey Dee and Rocky would be killed immediately.

Corky further advised DeCavalcante that the New York City Police Department was aware that Frankie Cocchiaro⁴⁸ was staying in Long Branch, New Jersey. Corky said they told him that they planned to kidnap Frankie from Long Branch, New Jersey.

He further related that he had received a message from one of the detectives, Frank Collins, to meet him one night following his arrest. Corky said that Collins warned him that an F.B.I. Agent had told Lieutenant Jacobs, the Commanding Officer of the 102nd Squad that there was a contract out for Corky, Moe Katz and possibly one other individual. According to Corky, Collins said that Katz was suspected of cooperating with the police. (Pgs. 1540, 1547)

N. On February 17, 1965, Sam DeCavalcante and his cousin, Bobby Basile⁴⁷ were engaged in a conversation about their problems. Basile advised DeCavalcante that Lieutenant Jacobson of the New York City Police Department had been contacted by the boys. Rudy had advised that they had gone to see Lieutenant Jacobson. Jacobson told them: "We know the whole story about the furs, just give us back or throw some of the stuff in the street. Like the sables and the chinchillas—then the whole thing will be closed." Rudy said he told Lieutenant Jacobson, "I don't know what the hell you're talking about." To which the Lieutenant replied "Look, if you got any doubts about me, go see "Toddo" Marino.⁸⁸ He will vouch for me."

Basile stated that he told Rudy, "Stay out of this, don't ask nobody nothing". He advised Sam DeCavalcante that Lieutenant Jacobson is the same guy that was involved with Johnny Rizzo and was involved with Frankie Dapper and everything else. Basile expressed his opinion that Jacobson was looking to make a score for himself—. (Newark Airtel to Washington dated 2/24/65). (Pgs. 1292, 1293)

O. On April 6, 1965, Sam DeCavalcante was visited by his niece Donna and her husband Tom. Tom is a member of the Plainfield, New Jersey Police Department and is planning to take the promotion exam for Sergeant on the coming Saturday.

DeCavalcante called the Trenton, New Jersey Police Department and spoke with a Lieutenant Lane. DeCavalcante said his nephew was a member of the Plainfield Police Department and would like to take the Sergeant's exam. DeCavalcante explained that he would like to get some books for the nephew to study for the exam, which was scheduled for the coming Saturday. DeCavalcante then spoke with another person and Sam arranged to pick up this other person's notes that his nephew might use to study in preparation for the exam. (Pg. 1583)

14. That the BOSS of the FAMILY controls some Unions and has working agreements with other Unions and uses the Unions to get payoffs and other advantages for himself and/or his Family.

A. On November 12, 1964, Sam DeCavalcante had a lengthy meeting with his cousin Bobby Basile,⁴⁷ Frank Cocchiaro,⁴⁸ his Caporegima and Basile's partner, Bernie Furst.⁵⁷

They began a discussion of their records to establish relations with building contractors and the Building Trade Union Representatives. They indicated that the late Nickolas Delmore who preceded DeCavalcante as the Boss of the Family, had derived a regular income from acting as intermediary in payoffs made by Contractors to Union Officials who are willing to allow a job to proceed with non-union workers. DeCavalcante succeeded Delmore in this activity.

The following conversations ensued: Sam will stand for DeCavalcante, Bernie will stand for Furst, Bob will stand for Basile.

Bernie: "I was seeing some of those Union guys today. Sam, this is what they may still have coming on Joe Wolf—next to Joe Kuschener⁸⁸—on the job that backs up on Route 287."

Sam: "Yeah, well they got paid for that—well I paid them myself; those guys are nuts!"

Bernie: "Now, for Rutgers Village they settled that one while Nick Delmore was alive."

Sam: "Rutgers Village is where?"

Bernie: "That's Joe Wolf's¹⁰⁰ on Route 46."

Sam: "And Nick settled with them?"

Bob: "For the first section."

Bernie: "No, no for the whole job."

Sam: "See they collected themselves there. They were supposed to give Nick the money."

Bernie: "Wait a minute, I'm sorry, you're right, they made the deal themselves. There's a new section going on that job now, Sam."

Bernie: "Now right next door to Rockmeal, Sam, is a guy by the name of Ralph Levey.¹⁰¹

Sam: "We haven't done nothing with him."

Bernie: "He's partners with Joe Wolf that's Joe Wolf's job."

Sam: "That dese guys are working half and half, half union and half non-union. I don't know Joe Wolf's job next to Kuschener was paid for. That's the one where we had all the meetings—you wasn't in on them then."

Sam: "I pay them personally, in fact they hollered because Larry Wolfson⁸⁸ was in on it."

Bernie: "Now that ends Joe Wolf for that tract. Now Kuschener, Sam, in that one section they're giving him the best of it. They don't remember whether they got paid for 150, or 180, so we mark down 180."

Sam: "Kuschener? Next to Joe Wolf?"

Bernie: "Right."

Sam: "How much was paid there?"

Bernie: "Well, Sam, I'll have to go count the apartments, I'll go up."

Sam: "Go count the apartments over there. They got paid for everything except the last section, which is a hundred and thirteen apartments."

Bob: "How many apartments are there altogether?"

Frank Cocchiaro: "There are two sections."

Sam: "There's three sections, excuse me, Frank."

Bob: "We gave them one hundred and eighty on over here."

Sam: "Bobby, when Nick was still living, he paid them for the first section. I owed them for the section. And I gave them \$10,800.00 which included the Kuschener deal, Route 10 and Route 46. These people got paid for Camerata and highway 10 and 46."

Bernie: "Number 10 was Monroe Markowitz¹⁰²."

Sam: "Now they had \$10,800.00 coming so Nick died and that little runt—that Italian guy."

Bernie: "Joe Richard."

Sam: "Yeah, he said, 'Well Nick died. I guess we have to forget our money'. I said, 'Listen, you jerk, Nick didn't die—only his body is dead. You guys are going to get paid'. And by Christmas I brought them ten thousand, eight hundred dollars to take care of everything. I got some from the Contractors but I laid out the rest. So where do they have money coming for these jobs?"

Sam: "Over here at Joe Kuschener's they got coming 113 times 75. So that's about \$8,000.00."

Frank: "Do you give them \$75.00 an apartment, Sam?"

Sam: "For Joe Kuschener's, Nick made a special price. The first section was \$75.00 too."

Bob: "Oh they don't got it."

Sam: "No, they don't get it I'm telling you what the score is there. Nick gave them a special."

Frank: "Oh all right."

Sam: "Now Monroe Markowitz, if he started a new section, they got money coming there."

Sam: "They got paid from Nick on 150 apartments, \$3,750.00."

Sam explained how he has tried to satisfy the obligations Nick Delmore made prior to his death.

Bernie: "Now Kuschener he's got four hundred units on Vale Road."

Sam: "That's all right."

Bernie: "All right, he's also got six hundred units on Vale Road."

Sam: "That he hasn't given a dime. He's coming in here. I'll handle him."

Bernie: "Now Joe Wolf—on Vale Road. Remember, Sam where we went. We met Bobby Sarcone¹⁰³ there. Only the machine was there way in the back. You couldn't even find it. That one there, he's got over 300 up right now."

Bernie: "And of course the one on Lake Hiawatha."

Sam: "Okay, that's all for Joe Wolf."

Bernie: "Well that's all for that tract."

Sam: "Now what do you do with the other guys working that area."

Frank Cocchiaro: "And why don't you tell him that Kuschener's making his own deal."

Bob: "I told him already."

Sam: "He tried to make it."

Bob: "Didn't I tell you Bobby Sarcone balked."

Frank: "He gave him five hundred dollars and he threw it back at him, Sam."

Sam: "All right, how about these other people up there you were suppose to see."

Bob: "Who, Sam? Adler is union. Arcano is settled and Pivnik we couldn't do a thing with. Arcano makes his own deals but on the next section we got him."

Sam: "He makes his deals with who, Bobby?"

Bernie: "See, the union people took fifteen hundred dollars apiece, three of them from this guy Ponterra. The job was going along."

Cocchiaro: "You know I'd like to get those guys together that claim they didn't collect no money."

Sam: "Well ask to sit down with them. I know they're lying. You see what it is, Frank, Nick Delmore messed a lot of things up. Nick left me in Westfield. He owed \$6,000.00. I forgot how much we lost. I asked him, 'Where's the money?' He said, 'I don't know, did Larry take it? Well that's all there is, \$3,500.00.' Then he got mad, if I asked him for it. These guys think that they can take advantage—they say, 'Let it go union, we make more money.' Tony Provenzano¹⁰⁴ called me up the other day—anything I want I can have from him in the Teamsters. Call him direct, I got his private number."

They discussed the share that the Union Officials received at a previous Contractor payoff. Bernie Furst claimed Nick Delmore paid only 25%. Sam was inclined to split evenly, however, was willing to be swayed. (Pgs. 705–714)

B. On April 22, 1965, Sam DeCavalcante met with Bobby Basile,⁴⁷ Bernie Furst,⁵⁷ and Frank Cocchiaro⁴⁸ to discuss labor payoffs.

Sam said that he had \$6,000.00 to split up among some of their contacts. There was considerable disagreement as to who deserved payment. They decided among those who had to be taken care of were George Laufensberg, Mike Cacchio, a brick layer, Bobby Sarcone,¹⁰⁵ Pete Weber¹⁰⁶, and Jim Varley.

Bernie Furst related that he has been having a couple of problems, one is with a young mason named Penacone who is handling the Masonry work on a job being done in North Plainfield by Joe Wolf¹⁰⁰. They said that Penacone is afraid to stick his neck out to take a bribe. Bernie said they have arranged to make a down payment on a Cadillac convertible for Penacone's wife. DeCavalcante expressed considerable annoyance at Penacone for putting pickets on Joe Wilf's job. He ordered Bobby Basile and Bernie Furst to straighten Penacone out. (Pg. 1783)

C. On October 22, 1964, Sam DeCavalcante, Bobby Basile⁴⁷, and Larry Wolfson⁵⁸, met and discussed Unions. DeCavalcante instructed Basile that he wanted to know anything that Basile did with Unions or other people. DeCavalcante mentioned a contractor in North Brunswick, who was getting a little balky and he indicated that he was going to throw a picket line on that contractor the next day. He stated that the contractor was getting fresh with the Unions and he wants to do business direct. He instructed Basile to see Carmen and to insure that Carmen and his laborers would be with DeCavalcante. Wolfson assured him that the Masons would be with DeCavalcante because of their connections, since they are partners with Sam Rita and Al Rita. (pgs. 552, 553)

D. On September 9, 1964, Bernie Furst⁵⁷, Bobby Basile⁴⁷ and Sam DeCavalcante discussed union situations of interest to them. DeCavalcante wants John Glizzi told what Sam has interest in and also Glizzi is to be told that his head will be broken if he interferes with DeCavalcante. They discussed Kuschener⁹⁹ and Wilf¹⁰⁶ and how much money is owed by these individuals. DeCavalcante said a meeting on the next day would straighten this matter out and wants cash rather than checks. They discussed getting books for a Union. Marty Winters suggested that Bob Murphy, who is the brother of the former mayor of Newark, Vincent Murphy, be requested to get the Union books and he described the type of Union books that Murphy gave him. Winters said that these "comic books" can pass for Union membership books. Marty Winters called Bob Murphy's residence from Sam's telephone. (Pg. 377)

E. On December 11, 1964, Marty Winters visited Sam DeCavalcante and brought some Union Books. He told Larry Wolfson to have a name and address typed in on the books.

When told that more Union Books would be needed, Marty suggested that Sam call Robert Murphy¹⁰⁶, the Secretary of Local No. 24, and say that three men had lost their books. Marty mentioned that Murphy will do anything for a buck. Marty told Sam that he should have Steve call in and give Marty the name to be used on the books so that it can be given to Murphy. Larry Wolfson⁵⁶ suggested not to use his typewriter and Marty agreed that the letters are different from those typed on the book. (Pgs. 780, 784)

F. On February 26, 1965, Gaetano Dominick Vastola,⁸³ also known as Corky, met with Sam DeCavalcante. Corky is interested in organizing and unionizing some employees in New York City and had received an offer from Joseph Danzo,⁶⁰ also known as "Whitey", who had suggested that Vastola bring the employees of this company into Local No. 242 of the Warehouse Industrial Union located at 301 George Street, New Brunswick, New Jersey, which "Whitey" Danzo controls. Danzo arrived at the office and brought with him some Union cards which he gave to Vastola to distribute among certain employees of the plant in question. The cards apparently indicate willingness on the part of the employees to organize. The following conversation ensued: DeCavalcante is referred to as Sam, Danzo is referred to as Joe and Corky by that name.

Sam: "Now who's going to handle this?"

Joe: "I left everything with Sue Nunziato, the representative of Local No. 242. My sister answers the phone in the office and if a guy by the name of Nunziato or anybody calls from the shop and gives that name I know it's from that shop."

"Whitey" explained that in order to have Corky's Local appear legitimate they should first organize through an existing Local, namely Local No. 242. Then after about one month Corky can open his own office and the membership will be switched back to him, along with "a couple of other shops in New York to make it look good."

Corky: "I also said this, Sam. If this turns out to be a score—we shoot it in back here."

Sam: "Wait a minute. I like to talk about money first so there's no misunderstanding. What end do you feel Joe should get?"

Corky: "Twenty-five percent over here. Because there's two guys and myself over there. That's three of us to Joe so you're the fourth guy."

Sam: "Do you think that's right—to forget me?"

Corky: "Forget you?"

Sam: "Yeah."

Corky: "Well that's what I told Mike, but yeah. Let's make it five. I'll take 20%."

Joe: "Me too."

Sam: "All right. Joe, you're satisfied with 20%."

Joe: "Yeah, I'm satisfied."

Sam: "Now how about the dues there; what do the dues come in now?"

Joe: "I use the dues for his books, stationery, and to set him all up."

Corky: "What are the dues a month?"

Joe: "Well you can make yours \$5.00 but I only have four dollars here."

Corky: "And what is the initiation fee? Ah, but I'm going to waive the fee to set up the shop."

Joe: "Right. Then you could charge 25, 50, or 75 dollars, whatever you want. Why not get 10 now and anybody comes in after—25."

Corky: "Yeah, all right."

Sam: "Well how you going to make a score if you're cheap?"

Corky: "Well I'm going to make the score this way. When I sit down with the Boss, I tell him how much it's going to cost him in welfare, hospitalization, —and all that. Say a plant with two hundred and sixty people will cost them \$4,000.00 a month just for hospitalization. So all together I make a package out of it, I'll

say. 'It's going to cost a hundred thousand dollars a year. Let's cut it in half and forget about it' and walk away. I show them first what it's going to cost then how much I'm going save him by his walking away."

Sam: "Well you'll have to organize the plant so nobody else walks in there—then you wind up with the dues every month. That's \$300.00 a month. You could do that?"

Joe: "Sure he could give a solid contract for three years where he won't get hurt."

Sam: "Then you get a pay every year." (Newark letter to New York dated 3/17/65) (Pgs. 1435, 1436, 1437)

G. On March 19, 1965, Sam DeCavalcante met with two individuals in his office, first names Joe and Lou. They discussed John Riggi²⁵ and they discussed Union Delegates and Sam stated that he always wants to be advised before any picket lines are set up. He reemphasized he must know beforehand when they are contemplating setting up any picket lines. (Pgs. 1454, 1455)

H. On March 8, 1965, Larry Wolfson,⁵⁸ Sam's partner, and Sam DeCavalcante and Sam's cousin, Bobby Basile⁴⁷ met and discussed their mutual interest in Construction-Labor Field. Wolfson related that Bernie Furst⁵⁷ had told him that the F.B.I. had questioned one of the builders in the New Jersey Shore area concerning his use of Union labor and any force being applied to affect his employment practices.

Basile asked DeCavalcante to instruct Joe Sferra to "lay off" Tony Constanza. Basile said he had received a complaint about Sferra's²⁷ pressure through Pussy Russo⁷⁷.

Basile also asked permission to "give somebody trouble." He referred to one Mark Feldman and Wolfson pointed out that Feldman had once been arrested on a bribery charge and he may now be cooperating with the authorities. It was mentioned that Mark Feldman and Sam Halpern are partners in several ventures and Feldman may also have an interest in the construction at the Junction of Routes 9 and 34. Nevertheless, Sam DeCavalcante authorized Basile to give the trouble to Feldman, cautioning him to be careful.

Basile stated that as an example of the caution he exercises that he never meets Pussy Russo at the Surf. He always sees Russo at Russo's office on Apple St. in Red Bank, New Jersey. (Pgs. 1480, 1481)

I. On March 25, 1965, Sam DeCavalcante and his Underboss, Frank Majuri²⁶ discussed the details of a meeting that DeCavalcante had had the previous night with Carlo Gambino³³.

DeCavalcante was very concerned because he had been embarrassed before Gambino over a labor dispute involving Tony Grande¹⁰⁷ and Joseph Sferra,²⁷ a labor business agent and Cosa Nostra member. One day the previous week, Sferra had invited Majuri to ride with him to a construction job in progress somewhere in the Elizabeth, New Jersey area. Majuri stated he had no prior knowledge of the dispute nor of the persons involved.

On arrival at the job, Sferra began arguing with the job foreman, the Superintendent and with Tony Grande over what may have been a jurisdictional matter. Finally Sferra ordered work on the job to cease.

Grande, who is "with" Carlo Gambino, but who was specifically referred to as "not a friend of ours", complained to Gambino. At the meeting with Gambino, DeCavalcante apologized for the actions of his men whereupon Grande made a remark indicating that on future jobs he would conduct himself as he saw fit. This gave DeCavalcante the opportunity to seize the offensive and berate Grande for his lack of respect. Gambino then supported DeCavalcante's position.

DeCavalcante said he has specifically forbidden Sferra from taking any more independent action if he expects to keep his job as Business Agent, "Amico Nos or no Amico Nos." (Newark Airtel to Washington dated 3/26/65) (Pgs. 1493, 1495)

J. On June 10, 1965, Samuel DeCavalcante met with Mike Madalia¹⁰⁶ whom Sam identified as a person very knowledgeable

in Union affairs. DeCavalcante wanted an opinion from Mike concerning the removal of Joseph Sferra as Business Agent of Local No. 394 Hod Carriers Union, Elizabeth, New Jersey. With the help of Mike Kleinbert¹⁰⁰, Manager of the Union County Laborers Welfare and Pension Fund, DeCavalcante was able to influence the Executive Board of Local No. 394 to have John Riggi named as assistant Business Agent during Sferra's absence as a result of his injury. It was DeCavalcante's intention to make this substitution permanent.

DeCavalcante sought Mike Madalia's advice as to how John Riggi could best be put in the job as Business Agent. Madalia told him that following a reasonable period, Sferra should resign. Then within six months an election for a Business Agent must be held.

From the conversation, it appeared that DeCavalcante was using this meeting as a means of demonstrating to Carl Gambino that previous injustices against Gambino's people working in the Union are now a thing of the past. Mike Madalia is a Cosa Nostra member responsible to Gambino. He was present at the Majuri wedding party at the Essex House in Newark, New Jersey on May 23, 1965. A wedding guest list showed one Michael Mandaglio as being present at this wedding. In 1957, Michael Mandaglio was then a representative of Local No. 394 which operated out of the West End Club on 14th Ave. in Newark, New Jersey.

While DeCavalcante and Madalia were conversing, Lou Russo arrived and DeCavalcante introduced him as the new Labor Delegate from Plainfield, New Jersey. When Mike Madalia and Russo departed they promised to cooperate fully with DeCavalcante. (Newark Airtel to Washington dated 6/17/65) (Pgs. 2083, 2084)

L. On June 23, 1965, Sam DeCavalcante, Larry Wolfson⁹⁸, met with Sam Halpern¹⁰⁰ and Joe Wilf¹⁰⁰. Wilf and Halpern are building contractors in the Union County, New Jersey area.

DeCavalcante complained to Wilf and Halpern about their inability to supply him with Union Payoff money, after DeCavalcante has negotiated with various Union representatives for labor peace. DeCavalcante pointed out that he had paid out fifty-seven hundred dollars and fifty-eight hundred dollars to union representatives. Halpern promised DeCavalcante that they would repay him \$6,000.00 as soon as they received the mortgage money on the job. Wolfson asked Wilf and Halpern to pay Kenworth Corp. for the work that Kenworth did on a particular project and Halpern promised that Kenworth would be paid out of the mortgage money also.

DeCavalcante explained to Wilf and Halpern that when he "fixes" a Union Representative, they expect to be paid immediately and not have to wait until the job is completed. DeCavalcante told Wilf that he never billed them for incidental expenses, such as gifts, wining and dining. DeCavalcante said that any one of these twelve men could make trouble for him in revenge for him forcing them to take the picket line off the job.

DeCavalcante emphasized to Wilf and Halpern that they owe him money for his services and for the services of the late Nick Delmore¹, dating back to the time when Delmore became sick and subsequently died.

DeCavalcante added to Wilf and Halpern that certain Union Representatives and their New York "sponsors" are pressing DeCavalcante for money on the three thousand apartment units that Wilf, Halpern, and Joe Kuschener⁹⁹ were currently building. Wolfson said that a Mr. Bradley from New York had been giving DeCavalcante a real bad time recently about payoffs on the part of Wilf and Halpern's buildings programs. DeCavalcante interjected that the New York crowds' demands do not bother him as they have no right to demand anything in New Jersey.

Both DeCavalcante and Wolfson complained that they take all the risks in setting up these payoff deals with Union Representatives. Wolfson claimed that he would be ruined, if ever he was involved in any investigation of these payoffs or was brought to

Court and found guilty of "graft negotiations". DeCavalcante related that these Union Representatives usually contact him telephonically in his office and that DeCavalcante has no assurance that the phone they are calling on or the phore that he is using is not tapped.

Wolfson told Halpern and Wilf that the previous week one of the Union Representatives involved in their Parsippany Apartment project told Wolfson that Halpern and Wilf would have to pay \$100.00 a unit for labor peace. Wilf and Halpern use a certain percentage of non-union labor on their construction projects and prefer to use mostly non-union labor which is cheaper and for which they have to pay Union Representatives money to overlook this situation.

DeCavalcante told Halpern and Wilf that in the future he will make Union Representatives payoffs in three parts: one third before the job commences; another third before the job is almost half completed; and the final third before the job is completed. DeCavalcante said he will not pay any part before receiving the money beforehand and if Wilf and Halpern do not like this arrangement they should forget that they know him.

DeCavalcante pointed out to Wilf that all the Union Representatives on any particular job have to be paid off. If only one representative was paid off, then the others in jealousy would strike the job and cause much union trouble on the job.

Halpern assured DeCavalcante that Wilf and he were planning to give DeCavalcante \$5,000.00 each for payoffs on the 174 Garden Apartment units on one of the Plainfield, New Jersey jobs. DeCavalcante refused this \$10,000.00. He said that the deal he made with the Union Representatives on this job calls for a hundred dollars a unit or \$17,400.00. Halpern said this job was a fifty-sixty percent union and DeCavalcante should not have agreed to \$17,400.00. DeCavalcante then told Halpern that they did not tell him that they were planning to use fifty to sixty percent union so the deal DeCavalcante made will have to be honored, even if DeCavalcante has to pay \$17,400.00 or any part of it out of his own pocket. DeCavalcante told Halpern not to see him in the future is this should happen. Halpern and Wilf then reluctantly agreed to give DeCavalcante \$10,000.00 within the next two weeks and \$8,000.00 over the next two months to make up the necessary \$17,000.00. DeCavalcante said in the future they should keep him advised to the percentage of union labor that they have to utilize on any particular job.

DeCavalcante then told Wilf and Halpern that they and Joe Kuschener⁹⁹ may have to pay high to use non-union labor on the projects that they are building, including those in the Parsippany-Denville, New Jersey area. DeCavalcante said that Union Representatives want close to two hundred thousand dollars in payoff money for the building that Kuschener, Halpern and Wilf are or will be constructing.

DeCavalcante commented that he had stuck his neck out for Halpern and Wilf on an Edison, New Jersey job that they had. DeCavalcante claimed this job became so hot that the Edison Chief of Police⁹⁴ and the Police Director were personally observing it. DeCavalcante said strike breakers had been imported into Edison to break the picket line on this job and it would have been a big mess except for the fact that DeCavalcante made the deal which settled the trouble on this job.

DeCavalcante told Wilf and Halpern that he wants payoff money from them in the future as he asks for it and does not expect to be keep waiting. DeCavalcante said that any time they feel they can do better with someone else to arrange their payoffs for them, then they are welcome to stop seeing him. He added that he does not make a nickel on arranging these payoffs and the only way Wolfson and he are paid is by being allowed to do the heating-plumbing work on the projects for which he arranges the labor peace.

DeCavalcante asked them how many units they were building in the Parsippany-Denville area job. Halpern claimed two hundred units and DeCavalcante said he heard it was a more than

four hundred unit job and that they had completed four hundred units already. Halpern replied that this was not true. Halpern said the job originally was to be a 112 unit job for which Halpern had made a deal with Wolfson for \$11,000.00 in payoff money. Halpern said because of the increased number of units in this job that Wilf and he want to give DeCavalcante \$20,000.00 to buy labor peace for them in the Parsippany area.

DeCavalcante told Wilf and Halpern that he does not know if \$20,000.00 will be enough and since he had to leave he told them they would have to talk to him at a later date about the payoff money on this job which was referred to as the Myra Road job. Wolfson then reminded Halpern and Wilf that the Union Representatives want a hundred dollars a unit or twenty-five thousand dollars in payoff money for the Myra Road job in the Parsippany area. (Pgs. 2203, 2204, 2205, 2206, 2207)

M. On July 2, 1965, Sam DeCavalcante, John Riggi, his Caporegima, met with Leslie, and DeCavalcante told Leslie that Budney of the Executive Board of the Union that Budney and Leslie are connected with is going to bring charges against Leslie which may result in an investigation. The charges have to do with unaccounted for losses of money. Leslie replied he was aware of the foregoing and in reply to DeCavalcante's offer to help, Leslie said there was nothing that DeCavalcante could do for him in this matter.

DeCavalcante repeated his offer to help Leslie at any time because Leslie has done favors for both DeCavalcante and the Riggis, Emanuel⁹⁶ and John²⁵ in the past.

DeCavalcante also told Leslie that he had been told that Budney is a treacherous individual. Budney is a secretary of the union and DeCavalcante would have given Budney a beating if Leslie asked him to do so.

DeCavalcante related to Leslie and John Riggi of a meeting that he had with Jim McKnight over the Algro Mills strike. McKnight told DeCavalcante that the textile workers union did not sanction this strike and the employees of Algro will not listen to the union. The strike has been on for six weeks. DeCavalcante suggested one way to end the strike would be to attack some of the strikers with baseball bats.

DeCavalcante asked John Riggi and Leslie how Sam Cherico from Amboy, New Jersey, who is with the laborers union, is? Sgambati had hit Cherico over the head with a bat. DeCavalcante said he tried to save Cherico from this beating but was too late as the beating was administered before DeCavalcante could stop it. (Pgs. 2253, 2254)

N. On May 21, 1965, Monroe Markowitz¹⁰² contacted Larry Wolfson⁵⁸ concerning 240 units that he was building. Wolfson spoke about protection from the other union locals from New Brunswick and the fact that they want to save money. (Pg. 1889)

O. On March 18, 1965, Monroe Markowitz¹⁰² visited DeCavalcante and Wolfson. He stated that the boys up above do not think that Larry Wolfson is treating them fair in the contracting business. Markowitz is an attorney, as well as being in the contracting business. DeCavalcante said: "We are just as much in trouble as the people who accept the money." DeCavalcante added that he isn't putting any money in his pocket from this type of operation. DeCavalcante told Monroe Markowitz about a strike in New Jersey which he had either broken up or had set up and that someone came with presents for him and for the girls as a result of his action.

DeCavalcante asked Monroe Markowitz if he was running something on the job. To Markowitz's reply of yes, DeCavalcante then asked if he needed a little money. He mentioned about two points on the money. (Pg. 1442)

P. On May 7, 1965, Sam Reida visited Larry Wolfson at the DeCavalcante-Wolfson Office. Wolfson told Sam Reida that he owes \$64,000.00 on the Dartmouth village job alone. He said this job has a hundred and thirty-four units and a balance of \$57,818.00. Wolfson also mentioned the job at Plainfield Manor

and indicated that the amount owed was \$24,360.00. Joe Kuschener⁹⁴ was also present at this meeting. Both Kuschener and Reida are building contractors in the Union County, New Jersey area. Wolfson in their presence checked the accounts payable book and was advised by his clerk that the figures were not up to date but the accounts payable indicated \$70,000.00 was owed on one particular job. He then checked the Cedar Lane account and the Clover Leaf Queens Garden \$91,000.00. (Pgs. 1810, 1811)

Q. On June 14, 1965, Sam DeCavalcante had a discussion with Mike Kleinberg¹¹¹ concerning Joseph Sferra's³⁷ actions while he was the union delegate of Local No. 394. DeCavalcante stated that it was a good thing that Sferra's actions had not come out prior to the elections at Local No. 394 as it appears that Sferra had expended considerably more money than he should have from the Union funds without the Union Board's prior approval.

DeCavalcante is interested in finding a way that he can meet the minimum membership requirements for Local No. 394. DeCavalcante would like to be on the membership roles for the medical benefits and other benefits that membership in Local No. 394 is entitled to. (Pgs. 2136, 2137)

15. That Family Bosses are very much interested in Garbage.

A. Louis Larasso⁵ had been trying to interest his Boss, Sam DeCavalcante in the purchase or lease of some land to be used as a garbage dump. The land is located in Sayreville, New Jersey and has the advantage of being only a short drive from New York City by way of the Verrazano Bridge.

The owner of the land is National Lead Company and Louis Sisto, whose company is the United Excavating Company of 634 St. Georges Ave E., in Linden, New Jersey, would provide the bulldozers and other equipment. Larasso reported that the deal was to be made through Sisto and that the owner wanted an annual rent of \$1,000.00 per acre for fifty acres. DeCavalcante felt that they should not commit themselves to a fifty thousand rental and suggested they pay the owner fifty cents for each load that was dumped.

On February 24, 1965, DeCavalcante reported the results of a meeting that he had with Carlo Gambino³³ about this garbage matter. He said that Gambino controls the garbage disposal in "all the boroughs" of New York City. At the present time it is necessary for Gambino to have all the garbage trucked to Long Island and Gambino was very enthusiastic about the prospect of using a dump in nearby New Jersey.

DeCavalcante outlined Gambino's thinking which would be that the two Bosses would share equally in the venture dividing their profits with their respective men. DeCavalcante opposed having any other partners, such as Sisto and the land owner. He said these two can be paid a flat amount and the balance of the profits will then go to Gambino and himself. He also suggested that Gambino's men have bulldozers and they want to use them instead of using Sisto's bulldozers. DeCavalcante spoke of a gross profit which could run to \$500.00 per day.

On February 26, 1965, DeCavalcante, Frank Majuri,²⁶ Lou Larasso,⁵ Nick Nelson⁵⁰ (whose true name is Nicola Melillo) and Jimmy Brown,⁵¹ (whose true name is James Failla) met and discussed the garbage deal. The New York representatives were only concerned with the travel time from New York. DeCavalcante suggested they inspect the garbage dump site and measure the distance over the various routes. They favored the payment of fifty cents per load to the land owner rather than a percentage in which in no case should it go over 15%.

The New York representatives opposed enlarging the partnership beyond DeCavalcante and Gambino. All were agreed that there is considerable money to be made in this garbage deal and spoke of a volume between 100 and 200 truckloads per day.

Larasso stated that the land owner is the president of a company which he did not name. This individual had obtained an industrial waste permit but has been unsuccessful in obtaining a

garbage permit. Larasso was informed that a garbage permit is essential and was directed to follow this matter very closely.

At the conclusion of this discussion, the New York representatives said that they would be meeting soon with Carl Gambino and that he would be in touch with Sam DeCavalcante. (Newark Airtel to Washington dated 3/4/65) (Pgs. 1341-a, 1341-b)

B. On February 25, 1965, Louis Larasso identified to Sam DeCavalcante the president of the company which owns the land which they hope to use in the garbage deal. He stated that this individual's name was Ralph Pizer. (Pgs. 1335-c, 1335-d)

C. On March 9, 1965, Lou Larasso⁵ advised Sam DeCavalcante that he had heard that Carl Gambino,³³ Joe Bandy³⁶ (true name Biondo), Joe Zingaro,³⁷ Nick Melillo,⁵⁰ and Jimmy Failla⁵¹ were in partnership in the garbage business in Mt. Vernon, New York. Included with them was one Joe Fiolo.⁵² DeCavalcante said he was aware of this and planned to ask Carl Gambino if he knows that Brandy, Zingaro, and Fiolo are connected with the deal. Larasso expressed some resentment, saying that if it was true, the Gambino participants far outnumber those from DeCavalcante's family and he felt they should be watchful that they are given their fair share of the proposed garbage deal.

Larasso told DeCavalcante that Joe Fiolo has repeatedly telephoned him concerning a garbage deal. Fiolo has a brother or a brother-in-law in the garbage business in New Jersey and wants Larasso to enter a partnership with this person. Fiolo has been contacting the Ford Motor Co., in Metuchen, New Jersey and eventually expects to secure this stop for Larasso and Fiolo's relative to pick up garbage. Fiolo expects Larasso to locate a suitable dumping site. Larasso has been putting Fiolo off until he could consult with DeCavalcante. DeCavalcante told Larasso that he would see Carl Gambino about Fiolo's proposition but that in the meantime Larasso should continue to stall Fiolo diplomatically. DeCavalcante added that he has heard that Fiolo is in trouble with Carl Gambino since Fiolo has been accused of stealing garbage customers from Joe Columbo. (Pg. 1712)

D. On March 1, 1965, Lou Larasso⁵ reported to Sam DeCavalcante that on February 27, 1965, he had taken James Failla⁵¹ and Nick Melillo⁵⁰ with him to see the president of the company which owned the proposed dump site. Larasso said the whole deal was negotiated to everybody's satisfaction. The property will be leased for ten years with a ten year option contingent upon Ralph Pizer being able to secure a garbage permit from the city of Sayreville. They anticipate no difficulty in this respect since Pizer is a very influential man in the community and has already laid the ground work. The first year, the leasing company will receive 40 cents per load dumped with a \$5,000.00 minimum. Then, if the operation is profitable, the fee will go to 50 cents per load for the remainder of the lease. In addition, as a "Commission", Pizer and Louie Sisto will receive together 35 cents per load.

Larasso added that both the New Yorkers were very enthusiastic over the deal and the meeting adjourned until their respective lawyers could get together on the next week. (Newark Airtel to Washington dated 3/15/65) (Pgs. 1407, 1408)

E. On April 9, 1965, Louis Larasso⁵ discussed the pending garbage dump arrangements with Sam DeCavalcante. The property is owned by the National Lead Company in Sayreville, New Jersey. DeCavalcante told Larasso that the Chairman of the Board of National Lead Company, Mr. Fishman has removed the President, Ralph Pizer, and Fishman wants to handle future negotiations himself. Although Fishman is more friendly than Ralph Pizer, Fishman's terms as set forth in a meeting between a lawyer and Nick Melillo⁵⁰ in New York were not as generous. Fishman wants a fee of \$5,000.00 plus an unstated sum per load dumped, with a guarantee of \$10,000.00 per year.

Larasso was very perplexed that the deal could take such a turn, after everything had been going along so smoothly.

DeCavalcante briefed Larasso on him meeting with John Riggi,²⁵ on the day before. DeCavalcante said he intended to ap-

proach Carlo Gambino³³ concerning purchase of some property in Carteret, New Jersey if only to stifle competition. DeCavalcante felt that his position might lead Carl Gambino to suspect him of duplicity if Gambino found that one of DeCavalcante's men, namely John Riggi, had gone into a similar type operation. (Pg. 1727)

16. The the Boss of the Family has contacts with legitimate Business world which permit him to use influence in placing people in positions.

A. On April 7, 1965, Sam DeCavalcante was visited by Sal Caternicchio³⁹ and his nephew, a singer, whose professional name is Nino Rossano. His true name is Giacobee. Rossano is twenty-four years of age and lives with his parents at 437 Spencer Street, Elizabeth, New Jersey. Sidney M. Flanzblau,⁵⁶ also known as Cris, attorney for DeCavalcante was present to draw up a contract between DeCavalcante and the singer. Rossano has been taking voice lessons from Carlo Menotti at the Carnegie Hall Studios. He has never made a personal appearance although Sal has assured DeCavalcante that he can sing better than Robert Goulet.

The terms of the contract will provide that DeCavalcante will pay Rossano's singing lessons, certain expenses, plus \$40.00 per week in return for 55% of all of Rossano's earnings, if any. DeCavalcante plans to meet with Maestro Menotti to work out the fees. DeCavalcante cautioned Nino Rossano that from then on he is not to make a move without advising Sal and/or DeCavalcante. (Pgs. 1675, 1676).

B. On June 23, 1965, Sam DeCavalcante was contacted by Celetti, who called concerning Nino Rossano, DeCavalcante's singer and discussed having an audition at National Broadcasting Co. in New York City. (Pg. 2132).

On June 25, 1965, Sam DeCavalcante and Harriet Gold,⁶⁴ his secretary discussed where they would meet in New York City that afternoon as they were going in to New York for a recording session for Sam's singer, Nino Rossano. (Pg. 2151).

C. On July 2, 1965, Sam DeCavalcante met with Angelo Felice. Felice is in need of a job. Felice has a law degree, is married and lives in New York City with his wife, Norma. He has never practiced law.

DeCavalcante asked Angelo Felice if he knew Joseph Profaci.¹⁵ Felice did know him but does not want to connect himself to any remaining Profaci relatives as Felice believes "the cops are constantly watching them". DeCavalcante also suggested that Felice see the Celano (phonetic) brothers but Felice declined, stating that he does not want to connect his name to those having continuous law enforcement attention.

On July 8, 1965, Sam DeCavalcante was contacted by Max Kendrick. Sam indicated to Kendrick that he has a friend who is a lawyer in New York and who was in the Italian film business. This individual lost out and wants to talk to someone. Max told Sam that he would see this person and Sam indicated that he appreciated this. (Pg. 2228)

Sam DeCavalcante sent Angelo Felice to see Max Kendrick of Warner Brother's Inc. on Madison Avenue in New York City. DeCavalcante told Felice that Kendrick is a contact of his and is handling DeCavalcante's singer, Nino Rossano. (Pg. 2256)

17. That the Boss and members of a Family are engaged in gambling.

A. On June 29, 1965, Sam DeCavalcante had a meeting with John Riggi²⁵ and Frank Cocchiaro,⁴⁸ both Caporegimes of his. John Riggi had recently learned that Shop Stewards of Local No. 394 pick up the numbers and horse action at the jobs assigned to them. Riggi went to Frank Majuri,²⁶ DeCavalcante's Underboss about this practice. Majuri told Riggi to continue doing this practice. However, Riggi brought this matter to DeCavalcante for Sam's opinion. Riggi feels that because he appoints the shop stewards and in the event of an investigation, which might uncover this practice, then Riggi would be arrested as the chief gambling figure behind the shop stewards.

Both DeCavalcante and Cocchiario told Riggi that he would not be affected if this practice became known to law enforcement authorities, because Riggi could claim that his only interest in the shop stewards was, if they did the Union work assigned to them. Riggi could show the shop stewards did their work and would be in the clear.

DeCavalcante warned Riggi to never "okay" anything illegal unless he knew that he could trust the individual asking Riggi's permission to do the illegal thing. DeCavalcante told Riggi that he did right by bringing this matter to his attention as DeCavalcante wants to know everything going on concerning Union Local No. 394. Riggi promised to inform DeCavalcante of everything that transpires in Union Local No. 394. (Pg. 2234-a)

B. On November 4, 1964, Jack Brennan and Larry Wolfson⁵⁸ had a discussion. Brennan told Wolfson that he heard there would be a game there. Wolfson warns Jack Brennan that they may have landed dice. Brennan is not worried. Jack wants to go with his partner.

Larry Wolfson⁵⁸ called Johnny Dubruen at the Old Orchard Country Club. Larry advised that he wants to make arrangements for some guests. Larry told Johnny Dubruen that Larry will be down later in the evening but wants the dinners charged to Larry's bill. Larry then asked Johnny if there would be a game tonight. It appears that there may be a friendly game. Larry Wolfson then made arrangements for a Jack Martin (true name Jack Brennan) and a Pat Russo (Brennan's partner) to get in the game.

Wolfson then warned Jack Brennan not to embarrass Larry Wolfson at the club. (pg. 559, 160)

C. On November 6, 1964, Sam DeCavalcante, Bobby Basile,⁴⁷ his cousin, and Frank Cocchiario,⁴⁸ DeCavalcante's Caporegima discussed the lease for the new corporation, Imperial, which is replacing the Mommouth Corp., which is now considered bankrupt.

DeCavalcante stated we may use the place for a drop for the numbers. DeCavalcante again mentioned that he may use that place for a numbers depot. Bobby Basile wanted to know if DeCavalcante is willing to pay \$300.00 a month for the place. (Pg. 572)

D. On June 23, 1965, Jack Brennan and Pat Della Russo visited Sam DeCavalcante. Jack Brennan mentioned to Sam DeCavalcante that Joe Columbo⁷ had closed up both his crap games in New York City. DeCavalcante said that Columbo was being followed all the time. (Pg. 2133).

E. On January 4, 1965, Bobby Basile,⁴⁷ Joseph "Whitey" Danzo⁶⁰ and Pat Russo visited Sam DeCavalcante. Danzo reported on their gambling venture. He said they had two hits on the numbers the week before last and none the last week. This week they have taken in over \$800.00, about \$490.00 of which is from Trenton area. Danzo noted that three of their best stops are presently closed, including the Ford Motor Company Plant in Metuchen, New Jersey. Danzo added that one of their last hits was by a truckman out of New Brunswick who stops in Elizabeth to buy a ticket. It was the second time that this person had won.

Sam DeCavalcante attempted to reach Joe LaSelva,²⁹ his Underboss, in Waterbury, Conn. but Joe was not available. The purpose of Sam's calling was to secure permission for Pat Russo to open a gambling activity in Joe LaSelva's area. (Pg. 990).

F. On January 22, 1965, DeCavalcante was visited by Tony Parisi who expressed his desire to start a bookmaking operation in Carteret, New Jersey. DeCavalcante instructed Parisi to "sit down with Pat Merola, who is with Joe 'The Indian' Polverino, trusted associate of Angelo Ray DeCarlo,⁴² in order to reach an agreement concerning the Carteret business". (Pg. 1102).

G. On April 21, 1965, Sam DeCavalcante, Joe "Whitey" Danzo,⁶⁰ and Kenny, a former dealer at the Sands in Las Vegas were discussing playing cards and the proper way of dealing, using plastic cards. Kenny mentioned keep two at the bottom bringing up one at a time, watch this. Kenny showed Sam how to

stack a deck, dealing from the bottom. He discussed Blackjack, Stud Poker, etc. DeCavalcante mentioned setting up someone for a game. He told Ken to make less moves as possible in the beginning then give it to him. They discussed switching of cards when reaching for change. Mentioned beating the other player with a little better flush. Kenny stated that he is a very fast dealer and will not be noticed. Kenny also mentioned craps and making few passes with dice. "Whitey" Danzo mentioned "Have you got anyone else to play with us." Sam stated he would let them know when he is ready. He said he would like to grab this guy about three times a year, it would be equal to a year's pay. (Pgs. 1716, 1717)

H. Joseph Danzo,⁶⁰ also known as "Whitey", had made arrangements with Sam DeCavalcante for Pat Della Russo to get into a crap game in Plainfield, New Jersey area. Pat is considered to be an accomplished "bust-out" man.

On April 12, 1965, Pat Della Russo reported to Sam DeCavalcante that he never entered this game because it had been raided on the Saturday before. (Pg. 1747)

I. On April 16, 1965, Joseph "Whitey" Danzo⁶⁰ and Ken visited Sam DeCavalcante. Ken demonstrated his card dealing ability to Sam. Danzo cautioned him to take his time. "Whitey" urged Ken to show Sam a few things he could do since DeCavalcante has seen the best. Ken specializes in Blackjack and can peak very rapidly. Ken and "Whitey" Danzo have developed a set of signals by which Danzo sitting to Ken's right can cut the cards according to Ken's wishes.

DeCavalcante has a "Pigeon" in mind and wants Ken's services. He stipulated that Ken should hit him big right at the beginning and let him try to recoup. Danzo was confident that Ken would have help in the game. Sam said he sees no problem since "Whitey" looks legitimate and can even speak Jewish.

Ken is also a dice specialist. He demonstrated that he can shoot any number he wants and in any combination.

DeCavalcante will get in touch with Ken through "Whitey" Danzo. Danzo will get the "sticks" (shills). Ken has one in mind, who is six foot three and looks like a yokel. This individual speaks Jewish and is from Brooklyn.

"Whitey" Danzo and Sam cautioned Ken not to tell anybody of their relationship. To this Ken agreed. (Pg. 1782).

J. On March 12, 1965, Bobby Basile⁴⁷ met Sam DeCavalcante. Basile gave Sam DeCavalcante some part of a \$400.00 score that he and Joseph Sierra²⁷ had made by forcing a small Elizabeth, New Jersey bookmaker out of business. (Pg. 1585).

K. On June 28, 1965, Tony Bananas⁷⁸ and "Blackie" Guiliano visited Sam DeCavalcante.

Tony Bananas was explaining how he runs his gambling enterprises. Tony Bananas stated that he has several people on his payroll at "a yard and a half (\$150.00) just to hang around". He said that even if he gets \$25,000.00 in the kitty nobody get a \$5,000.00 score. Bananas stated that he felt it much more practical to see that his men get a payroll each week rather than cutting up a large sum at irregular intervals. As an example, Tony Bananas stated that he has eight men handling the "twin double" and even though at one time they had \$20,000.00 in the kitty, each man drew \$150.00 a week.

DeCavalcante said "I'll come and be your man instead of being Boss, because I don't wind up with a yard and a half a week". (Pg. 2201).

18. That the Boss and members of a Family are engaged in Loan Sharking (shylocking).

A. On October 15, 1964, Sam DeCavalcante told his partner Larry Wolfson⁵⁸ that he, DeCavalcante, receives \$24,000.00 interest a year from one individual. (Pg. 467).

B. On October 14, 1964, Bobby Basile⁴⁷ told Sam DeCavalcante that Izzy Harris used to run to Little Pussy Russo⁷⁷ for money, but cannot run to Pussy Russo anymore. Bobby said that Izzy owes Pussy eight thousand dollars and has paid Russo about twenty thousand dollars. Bobby Basile stated that he expects to receive between seven and eight thousand dollars. (Pg. 456).

C. On October 15, 1964, Sam DeCavalcante had a lengthy meeting with Joe Kremer⁴¹ and Jack Kirsch,¹¹² both accountants. They went over DeCavalcante's Income Tax returns very carefully, attempting to justify DeCavalcante's past attestations for the years 1961 thru 1963. Jack Kirsch roughly computed that DeCavalcante's expenditures have been about \$18,000.00 a year whereas he was reporting income of only \$13,000.00 in 1961, \$10,000.00 in 1962, and \$11,000.00 in 1963. Kirsch pointed out that the government is also aware of these facts. With the possibility that Sam borrowed from various relatives, DeCavalcante is still about \$3,000.00 per year short.

DeCavalcante said that the Government believes him to be a shylock and in 1961 had raided a house he owned in Trenton, New Jersey. This was the beginnings of his trouble. DeCavalcante was accused of being a "Mafia member" and having entertained Mafia members in his home.

DeCavalcante noted that when he came to Kenworth Corp. he was "lame" (financially) because he had to support too many people. Since then he has become "respectable", the hangers on no longer can get to him and his losses have been cut 90%. Even his shylock loans have improved. He said he receives \$24,000.00 per year from one person and \$10,000.00 from another person in "interest" alone.

Harriet Gold,⁹⁴ his secretary, became alarmed lest Sam DeCavalcante be overheard, and suggested that the T.V. be turned on. DeCavalcante noted that he had implicit trust in Larry Wolfson⁹⁸ and her, saying he regards them as his brother and sister. Wolfson rose to the occasion with appropriate expressions of affection.

Wolfson remarked that he would try to get DeCavalcante to withdraw from the shylock business since he was trying to do too much. He wondered if "Frank from Brooklyn"⁴⁸ (Frank Cocchiaro) could assist Sam in this endeavor. DeCavalcante cryptically described himself as "a maker of monsters". Wolfson then suggested that DeCavalcante quickly vetoed Brennan, stating that he is not of Sicilian extraction.

DeCavalcante asked Harriet Gold to make a note of the fact that Joe Maglie⁵⁴ (true name Migliazza) owes him \$12,000.00. (Pgs. 544, 545, 546)

D. On November 11, 1964, Sam DeCavalcante and Bobby Basile,⁴⁷ his cousin, discussed an individual, named Peter, who has been testing DeCavalcante's patience by refusing to pay a debt that he owed to DeCavalcante. Sam DeCavalcante considered sending Frank Cocchiaro⁴⁶ and Corky⁶³ to see this delinquent. He also thought he might shoot a couple of blanks at this debtor in an effort to scare him.

Basile indicated that Carmine Rizzo had swatted him around in an effort to collect money, but due to Carmine's ineptness he was unable to do so. Basile predicted that Carmine might end up killing this debtor.

Basile then asked DeCavalcante, "So what are you going to do with Peter?" Basile asked if it were not true that Sam had swatted this guy around a couple of times. DeCavalcante acknowledged that he had, in fact claimed to have hit him across the face with a pistol, breaking his teeth.

Basile then asked Sam if he had heard from Joe⁵⁴ from Easton, Pennsylvania. DeCavalcante said that he had not and suggested that Bobby and Frank Cocchiaro travel to Easton and collect a debt that Joe Maglie owes to DeCavalcante. Sam authorized Basile to "talk to him any way you want". (Pgs. 640, 641)

E. On November 12, 1964, Bobby Basile⁴⁷ and Frank Cocchiaro⁴⁶ were instructed to contact Joseph Migliazza⁵⁴ in Easton, Pa. to collect some money that Migliazza owed DeCavalcante.

Basile has had this assignment for some time but was repeatedly stalled by Migliazza. Basile told DeCavalcante that Pat Russo had been in touch with Migliazza and had delivered \$480.00 from him on November 11, 1964. Basile explained that he had given Russo a message for Migliazza that he would tolerate no further delay.

DeCavalcante decided that Cocchiaro should accompany Basile to Easton on November 16, 1964. He instructed that Basile and Cocchiaro were also to contact Toto (true name Joseph Thomas) who he said has owed \$700.00 for about one year. DeCavalcante is willing to settle this debt for \$1,200.00.

Another debtor in Easton was identified, as that kid with taxi cabs, who may be related to Joseph "Fats" Koury. DeCavalcante said this person owes him \$3,600.00. He said Basile and Cocchiaro might have to rely on Migliazza to locate this person. However, under no circumstances were they to allow Migliazza to collect this debt for them. He instructed them that if Migliazza refused to produce the debtor, the thirty-six hundred dollars would simply be added to Migliazza's account of money owed.

DeCavalcante was also owed \$300.00 by "Toto's brother-in-law". Basile was told to advise this person that the debt is now \$400.00, however, he will settle for \$350.00. (Pgs. 642, 643)

F. On November 25, 1964, Sam DeCavalcante had a discussion with Frank Majuri²⁸ and Bobby Basile.⁴⁷ Basile told DeCavalcante that Joseph "Whitey" Danzo⁶⁰ is up before a Labor Board on some kind of union trouble. DeCavalcante asked if Bobby or "Whitey" had collected any money from Beneno at the Friendly Inn. Bobby Basile told him that he had gone to the Friendly Inn and spoke to Beneno's father about his son owing DeCavalcante \$3,500.00 and "Whitey" \$4,000.00. Beneno's father told Basile that he won't pay any debts owed by his son and he does not care if they "kill him". (Beneno)

DeCavalcante told Basile and Majuri to again visit the Friendly Inn with "Whitey" and see Beneno's father. Basile said that they would be wasting their time, but DeCavalcante said he wanted Beneno's father to tell Bobby he didn't care if they killed his son in front of Frank Majuri. DeCavalcante said that "Whitey" owes him \$4,000.00 and he is willing to take \$6,000.00 dollars from Beneno to settle both debts and Basile should tell Beneno's father this also.

Frank Majuri told Sam DeCavalcante that Ben Okin owes a kid "Majuri has" \$13,000.00 in shylock. Majuri said he heard Okin owes another fellow \$10,000.00 and a third fellow \$8,000.00. Majuri mentioned "his kid" has \$68,000.00 in shylock out on loan. Bobby Basile mentioned he had seen Tony Costanza and Costanza said that Okin had told him recently that he was going to see DeCavalcante. Costanza said that Okin wanted a favor but Costanza said Okin would have to see DeCavalcante first and obtain his permission for Costanza to do the favor.

DeCavalcante said that he is angry with Okin as Okin has been telling people that DeCavalcante is the big labor fixer in New Jersey. DeCavalcante said he saw Carl Gambino³³ in New York about Okin at one time and neither of them have seen Okin since. The last time DeCavalcante saw Carl they discussed Okin and Gambino said he is not partners with Okin in any deal. Gambino said that Okin used to consult him on labor trouble that Okin was having and Gambino advised him. DeCavalcante said he asked Gambino if he was giving Okin advice on how to deal with the labor trouble Okin was having in Elizabeth, New Jersey but Carl Gambino said he was not, because he knew that DeCavalcante would not like him to do so.

DeCavalcante asked Bobby Basile if "Whitey" Danzo had collected any money that the kid from Colonial owed them. Basile said "Whitey" had not and DeCavalcante became angry at "Whitey" and Bobby because of this. Basile placed the blame on Danzo and said it is hard for Basile to see "Whitey" Danzo and tell him that DeCavalcante wants the debt owed by this kid from Colonial settled.

DeCavalcante then told Basile and Majuri that Art Mastrapeter had seen him recently. DeCavalcante explained that Mastrapeter is an undertaker on Elizabeth, who owed money to the accountant, Jack Kirsch,¹¹² who is Jerry Catena's and Carmen Battaglia's friend. DeCavalcante said that Mastrapeter was shaking and promised to sell his boat and his Cadillac to raise

the money to pay the debt and would bring the money to DeCavalcante on November 30, 1964. (Pgs. 811, 812)

G. On March 12, 1965, DeCavalcante attempted to contact an individual in Florida but was unsuccessful. He then told Harriet Gold⁶⁴ that he had just completed a shylock deal which will pay off six thousand dollars by Christmas 1965. DeCavalcante promised Harriet Gold that he would give her 20% of the amount of money he makes on this deal when it is culminated at Christmas. (Pg. 1539).

H. On March 15, 1965, Sam DeCavalcante and Izzy Harris, Bobby Basile,⁴⁷ and Bernie Furst⁵¹ met. DeCavalcante told Izzy Harris that he had arranged a \$10,000.00 loan repayable at \$250.00 a week for fifty weeks for Izzy. DeCavalcante said he was doing this as a favor and he will not receive a dime. The money will be available by either Tuesday or Wednesday. DeCavalcante warned Izzy Harris not to tell anyone about this loan. DeCavalcante then inquired as to how Izzy Harris was going to get this money into the bank. Basile said that he will make arrangements and has already taken care of these arrangements. (Pg. 1630).

I. On January 23, 1965, Lou Larasso⁵ told Sam DeCavalcante of an individual who was trying to borrow fifty thousand dollars and is willing to pay ten thousand dollars interest for six months. He had mentioned this matter previously. DeCavalcante instructed Larasso to get the prospective borrower's address from Larry and take him to Frank Perrone's office where they will meet with Frank and Tony. They will advance the loan, if they see fit and if they do, then Sam DeCavalcante will receive 1% of the profits from Perrone. (Pg. 1100)

J. On June 14, 1965, DeCavalcante and Bobby Basile⁴⁷ discussed Joe Manno who owes \$4,800.00 to DeCavalcante for gambling losses. Basile has been negotiating with Manno. Manno would like to settle this debt for two thousand dollars but Basile knows that DeCavalcante wants this debt paid in full. DeCavalcante told Basile to tell Manno to meet with DeCavalcante. Basile is to tell him also to bring the \$2,000.00 as part payment of his debt. Manno has some connection with Pussy Russo,⁷⁷ but Pussy won't help Manno in this matter. (Pg. 2115)

K. On January 6, 1965, Jack Brennan and his associate, Pat Della Russo visited DeCavalcante. DeCavalcante was critical of Pat Russo for failing to report earlier some difficulty he was having with some "connected" people in his Brooklyn neighborhood. Pat said that he had been approached by one Sally Daniels, whom he believes to be associated with Johnny Burns.¹¹ Daniels claimed to represent one Sally Paluggi who was demanding the immediate payment of \$1,000.00. This \$1,000.00 debt was allegedly lent to Pat's father, now deceased. Pat Russo stalled as long as he could, claiming he owed Paluggi nothing, his allegiance being to DeCavalcante. Daniels disputed this and finally threatened that unless the debt was paid, he would personally find a way to kill Pat.

Jack Brennan interjected that Daniels has previously tried to muscle in on him and Pat in their gambling activities.

During this conversation, DeCavalcante received a telephone call and immediately repeated the caller's number as 212 JA3-9784. He said that he would call back in two minutes, hung up and announced that it was Johnny Burns and that he was going to the public telephone to call Burns back.

When DeCavalcante returned he quizzed Pat Russo closely to assure himself that Pat had never accepted any favors from Daniels, namely had Daniels ever "married" him. Pat said that Daniels once offered him protection in return for a percentage of his earnings, but Pat refused at the time and has never paid Daniels since. When Pat mentioned that this Sally Paluggi was behind it all, DeCavalcante said, "That's not his name anyhow."

Later DeCavalcante's Underboss, Frank Majuri arrived and was briefed on the situation. DeCavalcante told Majuri that he has spoken with Johnny Burns and feels the matter will be settled. Majuri cautioned Pat Russo not to get in a car with anyone

and to decline all offers to talk about the matter, with the story that he is on his way to see DeCavalcante. After Jack Brennan and Pat Russo left, Majuri replied: "It must be Sally Burns, (True name Rosario Morales)" (Pg. 987, 988)

19. That the Boss tries to insulate himself from possible Criminal Prosecution—Is concerned about security

A. Boss fears that his phone is wired (bad). On September 25, 1964, Sam DeCavalcante was joined by Bobby Basile.⁴⁷ The following conversation ensued. DeCavalcante identified by Sam, Basile identified by Bob:

Sam: "Remind me to make that call from New York."

Bob: "Call Joe."⁵⁴

Sam: "Joe who?"

Bob: "From Easton."

Sam: "I don't want to call him now."

Bob: "Why, his house is bad?"

Sam: "This may be bad." (Referring to his own phone.) (Pg. 311)

B. On October 9, 1964, Sam DeCavalcante and his cousin, Bobby Basile⁴⁷ were visited by an unnamed male who told Sam that he was supposed to hear from a Joe. The name Bananas was mentioned. Sam DeCavalcante wanted to know what was he supposed to talk to me about? The unnamed male did not know. The radio was then turned on very loud. Bobby Basile tells the visitor, "Let's go outside and call this Joe."

Sam DeCavalcante told Bobby, "Call from the gas station." The unnamed visitor states that Joe is a bookie and works with the Gallo branch of the Profaci¹⁵ family. (Pgs. 322, 323)

C. On October 2, 1964, Sam DeCavalcante and his cousin, Bobby Basile⁴⁷ were discussing the delinquent accounts of Joseph "Whitey" Danzo.⁶⁰ DeCavalcante's patience is at an end and he ordered Bobby to collect the money wherever he can. Sam told Bobby to bring him to his office as he wanted to make a few phone calls. Sam then said, "Come on, let's get out of here. I thought I said keep out of this place, I don't even like to go to that phone." (Indicating the phone in his own office). (Pgs. 343, 344)

D. Later on October 2, 1964, Sam DeCavalcante and Bobby Basile⁴⁷ returned to Sam's office. DeCavalcante directed Basile to turn on the radio. DeCavalcante then made some remarks about his future, the essence of which was that he does not want to take too many chances which might result in his arrest. He said he has been courting Harriet Gold,⁶⁴ his secretary because she knows too much about him. Bobby cautioned against this citing the fact that Vito Genovese's wife betrayed him and that if a wife could do this, a girl friend would be more apt to do so.

At this point the inter-office buzzer sounded and Bobby answered it. He learned that John Riggi²⁵ was waiting to see Sam. Basile then said, "Now you see that's bad. I'll tell you why, because if this phone is wired, the intercom is wired too." Basile explained to DeCavalcante that his greatest danger lies in his exposing himself to legitimate businessmen who would not feel compelled to keep quiet about it. He named Eddie Piskayvich, a trucker who doesn't owe enough money for Sam to risk a direct contact.

Basile then stated, "You talk to Tony Costanza on the phone! Sam, that phone is wired—who are you to be talking to businessmen? If you want to talk to Tony Costanza, I can handle him for you! Save yourself for the big ones!" (Pg. 346).

E. On September 16, 1964, Bobby, Basile⁴⁷ asked his cousin, Sam DeCavalcante, if he knew that Joey Columbo's⁷ office was wired, Basile added that they got recordings of everything. He stated that they made that discovery, it goes to a house across the street. (Pg. 354).

F. On February 25, 1965, Frank Cocchiario,⁴⁸ DeCavalcante's Caporegima expressed his annoyance at Corky Vastola's⁸³ attempt to collect thirty-five hundred dollars debt from Mikey Dee,⁶⁹ their partner in a fur theft. In his indictment of Vastola, Cocchiario said that he had a slight suspicion that

Vastola might be a stool pigeon, based on the fact that the police were around Cocchiaro's house when only Vastola knew that he had returned from Florida.

On February 26, 1965, Corky Vastola contacted Sam DeCavalcante. Vastola convinced DeCavalcante that he was guilty of no misbehavior and in addition was perfectly justified in demanding repayment from Mikey Dee.

Vastola said that he had received a message for Cocchiaro from a Jimmy Rotunda. According to Rotunda, Frank Cocchiaro should stay away for another two weeks. Vastola said, "That's what they had—Title 18, Sections 2314, 2315, and 1852. These were the charges that they want to hit Frankie Cocchiaro with. Stay away another two weeks and then they will have to erase the telephone tapes." Vastola did not elaborate on this last remark nor did he identify the source of Jimmy Rotunda's infor-

mation. (Pgs. 1394, 1395).

G. On September 14, 1964, Jack Panels⁹³ and Sam DeCavalcante were discussing security of Cosa Nostra. Sam said that Basile had told him that the authorities had learned about two of his Caporegimas, they knew every move already. Panels related that he had been told that there was a notification in the newspaper column that Joey Columbo⁷ was to be "made" two days before it occurred. DeCavalcante replied that somebody told him the other day that among Cosa Nostra people there were stool pigeons. Jack Panels related that Albert Anastasia⁴¹ "made" so many men that F.B.I. Agents could have slipped in. And Panels stated that Ray DeCarlo⁴² feels there may be a couple of Agents right in Cosa Nostra.

Panels then said that in the past the organization was more secure. (Pgs. 241, 242).

A P P E N D I X

1. NICK DELMORE - Boss of La Cosa Nostra New Jersey Family. - Hearings before the subcommittee on Criminal Laws and Procedures of the Committee on the Judiciary, U.S.Senate - 91st Congress March 18, 1969 (Hereinafter cited as Hearings - 1969) at P. 126
2. ANGELO BRUNO - True full name ANGELO BRUNO ANNALORO, Boss of La Cosa Nostra - Philadelphia, Pa. Family - - ibid. at P. 128
3. IGNAZIO DENARO - Underboss of La Cosa Nostra - Philadelphia, Pa. Family - ibid.
4. MR. MAGGIO - Possibly identical to, or ancestor of PETER J. MAGGIO, capodecina. of Philadelphia, Pa. Family - ibid.
5. LOUIS LARASSO - Also known as "FAT LOUIS", La Cosa Nostra member from New Jersey who attended the Appalachian, New York, convention, 1957. Hearings before the permanent Subcommittee on Investigations of the Committee on Government Operations, U.S.Senate, 88th Congress (Hereinafter cited as McClellan Committee - Organized Crime) at P. 329.
6. JOHN "SONNY" FRANZESE - Capodecina in the JOSEPH COLOMBO La Cosa Nostra family cf. Hearings - 1969 at Pgs. 126, 127. Also McClellan Comm. - Organized Crime at Pgs. 308, 311, 652.
7. JOSEPH COLOMBO - Boss of one of La Cosa Nostra New York, N.Y. Families. Ibid at P. 126, Member of the Commission, P. 124. Op. CIT at Pgs. 308, 311, 652, 913.
8. JOSEPH BONANNO - Also known as JOE BANANAS, Deposed Boss of one of La Cosa Nostra - New York, N.Y. Families. cf - Hearings - 1969 at Pages 124, 127, 128. Also cf. McClellan Comm. - Organized Crime at Pgs. 88, 162, 166, 184, 246, 247, 313-315, 524, 652, 894, 897, 911, 912, 917, 923, 925, 929, 972, 1001, 1015, 1061. He was on the Commission..
9. GASPARINO DeGREGORIO - Also known as GASPAR - A Caporegima of the Joseph Bonanno, La Cosa Nostra Family.
10. JOSEPH ZERILLI - Boss of La Cosa Nostra Detroit, Michigan Family. cf. Hearings-1969 at Pgs. 125, 126. Also cf. McClellan Comm - Organized Crime at Pgs. 410, 411, 420, 425, 428, 431, 433, 434, 441, 444, 472.
11. JOHN MORALES, Also known as JOHNNY BURNS - Underboss of Joseph Bonanno.
12. GERADO CATENA - Also known as Jerry Catena, - Underboss of the Vito Genovese, La Cosa Nostra Family, and Acting Boss in view of Death of Genovese. cf. Hearings - 1969 at Pg 127. Also cf. McClellan Comm. -Organized Crime at Pgs. 179, 246, 248, 251, 253, 272, 293, 327-329, 912, 929, 1015, 1019.
13. JOSEPH ARTHUR ZICARELLI, also known as JOE BAYONNE, Bayonne Joe. - Caporegima in Family of PAUL SCIACCA, successor as Boss of Bonanno Family. cf. Hearings - 1969 at Pg 128 Also cf. McClellan Comm. - Organized Crime at Pgs. 912, 916, 1002, 1030, 1061.

14. JOSEPH MAGLIOCCO, also known as JOE MALYAK - was underboss under Family Boss Joe Profaci, and Temporarily succeeded as Boss on Profaci's death in 1962 until removed by the Commission. His death is alluded to in these transcripts. cf. Hearings - 1969 at Pg. 126. Also cf. McClellan Comm. - Organized Crime at Pgs. 7, 162, 246, 247, 308-310, 371, 373, 374, 376, 377, 652, 913, 917, 921, 930, 1036, 1061.
15. GUISEPPE PROFACI, also known as JOE PROFACI, "THE OLD MAN", deceased Boss of New York, N. Y. La Cosa Nostra family, currently bossed by Joe Columbo Ibid. at Pgs. 126,127.
16. JOHN LA ROCCA - Boss of La Cosa Nostra Pittsburgh, Pa. Family.
17. JOSEPH NOTARO, also known as "LITTLE JOE". Caporegima under Boss Joe Bonanno. cf. Hearings - 1969 at Pg. 127. Also cf. McClellan Comm. - Organized Crime at Pgs. 313, 314, 652, 1009, 1030, 1047.
18. VITO DeFILIPPO - La Cosa Nostra Member of Joe Bonanno Family.
19. THOMAS "Smitty" D'ANGELO - Caporegima under Joe Bonanno. cf. Hearings-1969 at Pg.127.
20. JOHN AQUARO - Caporegima under Joe Bonanno.
21. ANGELO CARUSO - Caporegima under Joe Bonanno.
22. CHARLIE BATTAGLIA - Caporegima in Arizona under Joe Bonanno. Brother of Carmen Battaglia, a feared, ruthless figure in Newark, N. J. La Cosa Nostra circles.
23. FRAN LABRUZZO - A Caporegima under Joe Bonanno, representing Montreal, Canada, area.
24. GENE CATENA -(T N EUGENE CATENA) deceased brother of Gerado Catena acting boss of the late Vito Genovese family. Gene Catena was caporegima and trusted Chief Lieutenant of Jerry Catena. cf. Hearings-1969 at Pg.127.
25. JOHN RIGGI - A Caporegima of Samuel De Cavalcante, Boss of the New Jersey Family of La Cosa Nostra. The Newark Evening News of July 8, 1969, described John Riggi, of Linden, N. J. as "an alleged 'fixer' of Union Activities and a member of the Linden Human Rights Commission. Riggi is an official of Local 394, Laborers International Union, Elizabeth, N.J."
26. FRANK MAJURI - Underboss of Samuel DeCavalcante, Boss of the New Jersey Family of Cosa Nostra. The Newark Evening News of June 22, 1969, Pg. 1, described Majuri as "A familiar figure in Organized gambling in Union County (N.J.) Majuri, with Larasso was a delegate at the 1957 Mafia convention at Appalachin, N.Y." cf. Hearings-1969 at Pg. 126. Also cf. McClellan Comm. - Organized Crime at Pgs. 329,970.
27. JOSEPH SFERRA, also known as JOE TIGER was appointed a caporegima and demoted by Samuel DeCavalcante, boss of the New Jersey family. DeCavallante also removed Sferra from his job as BusinessAgent of Local 394, Laborers International Union, Elizabeth, N. J.

28. MIKE PUGLIA, also known as MICKEY POOLE, a Caporegima in Connecticut for the DeCavalcante Family, serving under JOE LaSELVA, Co-underboss of the Decavalcante Family, responsible for Connecticut interests.
29. JOSEPH LaSELVA, also known as JOE LaSELVA, Co-underboss of the Samuel DeCavalcante Family, responsible for Connecticut interests.
cf. Hearings - 1969 at Pg 126.
30. PAUL FARINA - appointed caporegima by Samuel DeCavalcante to replace demoted Joe Sferra.
31. SAM MOONEY - True name SALVATORE GIANCANA, also known as SAM GIANCANI, ALBERT MASUSCO, SAM FLOOD; he was the Boss of the Chicago Family of La Cosa Nostra. Boss position probably deemed open now due to flight of Giancana to Mexico in 1966, after he spent approximately 1 year in confinement for contempt in refusing to testify after having been granted immunity. Was a member of the Commission. cf. Hearings - 1969 at Pg.124,125. Also cf. McClellan Comm - Organized Crime at Pgs. 504,508,513,516,524, 1069,1106,1115.
32. THOMAS LUCHESE - Also known as TOMMY BROWN, "THREE FINGERS", True name GAETANO LUCHESE. Deceased Boss of the Luchese Family, one of the 5 New York, N.Y. La Cosa Nostra Families. Was a member of the Commission. cf. Hearings-1969 at Pgs. 124,127. Also cf. McClellan Comm - Organized Crime at Pgs. 87, 88, 92,117,138,140,162,175-177, 216,226,230,246,274-282,284,285,288,294,296,353,359,360,652,894, 897,912,917,919,922,925,930,961,972,973,977,986,990,1001,1015, 1018,1020,1028,1029,1036,1044,1050,1057,1061.
33. CARLO GAMBINO - also known as DON CARLO, Boss of the Gambino Family, 1 of the 5 New York, N. Y. La Cosa Nostra Families. Is a member of the Commission. cf. Hearings-1969 at Pgs. 124,127. Also cf. McClellan Comm.-Organized Crime at Pgs. 81,82,88,117,162,189,246, 247,294,295,297,298,302,304-306,348-350,652,894,912,917,921,923, 924,926,930,982,994,1010,1028,1054,1061.
34. STEFANO MAGADDINO, also known as "THE BOSS", "THE OLD MAN". Boss of the Buffalo, N.Y. Family of La Cosa Nostra. He is also a member of the Commission. cf. Hearings-1969 at Pages 124,125. Also cf. McClellan Comm.-Organized Crime at Pgs.7,91,193,196,219,299,389,390, 580,582,586,587,588,589,592,595,596,597,599,601,602,603,605,606, 607,609, 610,611,612,613,783,912,916,930,991,1017,1023,1036,1062.
35. MICHAEL SAVELLA, also known as MIKE SAVELLA, "MIMI", A caporegima in the Paul Sciacca Family, 1 of the 5 New York, N. Y., La Costra Nostra families, which was previously known as the Bonanno Family. cf. Hearings-1969 at Pg 128. Also cf. McClellan Comm-Organized Crime at Pgs 313,314,652.

36. JOSEPH BIONDO, also known as JOE BANDY, JOE BANTI, CUNNIGLIEDDU - was an underboss in the Carlo Gambino family but was removed - demoted- by Gambino in 1965. cf. Hearings-1969 at Pg 127. Also cf. McClellan Comm-Organized Crime at Pgs 162,246,294, 295,348,349,652,772,876,891,894,910,912,924,929,972,974, 983,986,987,1006,1015,1029,1061.
37. JOSEPH ZINGARO - A Caporegima in the Carlo Gambino Family - 1 of the 5 New York, N. Y. La Cosa Nostra families. cf. Hearings-1969 at Pg 127.
38. PETER CASTELLANO - A relative of Carlo Gambino and identified by DeCavalcante as a Caporegima in the Gambino family, although not so identified in Hearings - 1969 at Pg. 127. cf. McClellan Comm-Organized Crime at Pg 302.
39. SAL CATERNICCHIO - a member of the DeCavalcante Family, New Jersey La Cosa Nostra family.
40. "DAYLIGHT" - Alias of MICHAEL SALVATORE TRAMANTANA - a member of the Angelo Bruno, Philadelphia, Pa. Family of La Cosa Nostra. He resides in Trenton, N. J., and reportedly has been used as strongarm man by Bruno.
41. ALBERT - ALBERT ANASTASIA - former boss of the Gambino Family, who was shot to death in a hotel barber shop in New York in 1957. cf. McClellan Comm. Organized Crime at Pgs. 7, 118, 162, 187, 237, 239, 256, 294,295,304,320,322,325,328,331,339,348-350, 362,379,380,388,524,525,534,652,912,917,980,1000,1047,1061.
42. ANGELO DE CARLO, also known as RAY DE CARLO, "GYP" DE CARLO, JOE DE CARLO, LARRY RYAN, LAWRENCE RYAN, RAY LAWRENCE, EDWARD MING. He is a caporegima in the Vito Genovese family, 1 of New York, N.Y. La Cosa Nostra families. He resides at and runs his operations from Mountainside, N. J. He is under Gerardo Catena. cf. Hearings-1969 at Pg 127. also cf. McClellan Comm-Organized crime at Pg 1019.
43. ANTHONY "TONY BOY" BOIARDO - is the son of Ruggiero Boiardo, also known as "THE BOOT". He is member of the Vito Genovese La Cosa Nostra family. He has been active in gambling, shylocking, illegal alcohol and spends most of his time at Valente Electric Co. which he ostensibly owns. This firm receives the awards on most of the Federal, State and Local Construction in New Jersey. cf. McClellan Comm.-Organized Crime at Pgs.248,326,328,652.
44. "CADILLAC CHARLIE" -Cadillac Charlie Cavallaro. cf. The Silent Syndicate by Hank Messick. Pgs. 217,218.

45. "THE BOOT" - True name RUGGIERO BOIARDO also known as RITCHIE, "DIAMOND RICHIE". - a caporegima in the Vito Genovese family, 1 of the 5 New York, N. Y. La Cosa Nostra Families. He resides on a large estate in Livingston, N. J. cf. Hearings-1969 at Pg 127. Also cf. McClellan Comm.-Organized Crime at Pgs. 248,256, 326, 328,652, 912,929,1015,1061. Father of Tony Boy Boiardo.
46. QUARICO MORETTI, also known as WILLIE MORETTI, WILLIE MOORE, CHICK MEYERS. Was a former Caporegima in the Genovese Family. He was murdered at 11:00am October 4,1951, in Joe's Elbow Room, Palisade Avenue, Cliffside Park, N.J. cf. McClellan Comm.-Organized Crime at Pgs. 149,156,248,279,296,324-326,328-331, 335,342,348,601,602,652,980.
47. BOBBY BASILE, True name ROBERT OCCHIPINTI, a blood cousin of Samuel DeCavalcante. He had not yet been "made" a member of La Cosa Nostra, but was a candidate. He and Cocchiaro were top aides and enforcers for DeCavalcante and also are officers in a legitimate company owned by DeCavalcante. Newark Evening News 6/18/69; 7/8,9/69.
48. FRANK COCCHIARO, also known as BIG FRANK CONDI, is a Caporegima in the Samuel DeCavalcante, New Jersey Cosa Nostra Family. He lives in Ocean Township, N.J. and was formerly a member of the Carlo Gambino Family. Newark Evening News 6/18/69,Pg 1; 7/8/69;7/9/69.
49. RALPH DeMEGLIO - also known as BIG RALPH is bodyguard and member of Bayonne Joe Zicarelli's Decina in the Paul Sciacca Family - 1of the 5 New York, N.Y. La Cosa Nostra Families.
50. NICK MELILLO - True name Nicola Mellillo, also known as NICK NELSON - a member of the Carlo Gambino Family.
51. JIMMY FAILLA - also known as JIMMY BROWN - a Caporegima in the Carlo Gambino Family. cf. Hearings-1969 at Pg. 127.
52. JOE FIOLO - A member of the Carlo Gambino Family who was in trouble with Gambino for stealing Garbage customers from Joe Columbo.
53. ANDY "HAM" DOLASCO - Deceased former member of the Tommy Luchese Family. He had been soldier-under the late PAUL CORREALE, also known as "PAULIE HAM" and later under PENOOKS (Pa) from Atlantic City, N. J. He was very active in gambling.
54. MR. MAGLIE - True name JOSEPH MIGLIAZZA, also known as "THE MERCHANT", a gambling figure in Easton, Penna. He owned a restaurant in Easton and arranged through BOBBY BASILE to have it burned so that he could collect insurance and pay off shylock loan owed DeCavalcante. He collected \$80,114 from Employers Liability Co. of Boston. He started serving a term in Federal Penitentiary at Lewisburg, Pa. on a gambling charge in December 1968. Newark Evening News 6/18/69 Pg. 10.

55. "PUSSY" - ANTHONY "LITTLE PUSSY" RUSSO. The Newark Evening News 6/18/69. Pg. 1, stated that Russo was known for several years as the late Vito Genovese's top captain at the New Jersey Shore. The domain was said to include all of Monmouth, Ocean and Middlesex counties. He wielded considerable power in Long Branch, N.J. He has close relationship with Angelo DeCarlo and might be under his control. His brother is JOHN "Big Pussy" RUSSO.
56. CHRIS FRANZBLAU - True name SIDNEY M. FRANZBLAU, Attorney for Samuel DeCavalcante, and a former Assistant U. S. Attorney.
57. BERNIE FURST - From Long Branch, not a La Cosa Nostra member but is a partner with BOBBY BASILE and FRANK COCCHIARO in the Imperial Air Conditioning, Long Branch, N.J. financed by DeCavalcante. Newark Evening News, 7/8/69/
58. LAWRENCE WOLFSON, also known as LARRY WOLFSON - not a Cosa Nostra family member but is partner of Sam DeCavalcante in Kenworth Corp. Kenilworth, N. J. He resides in Deal, N.J. in a \$100,000 home. He was associated with Nick Delmore before DeCavalcante took the reins. Newark Evening News - 6/18/69.
59. DANNY NOTO - A relative-cousin of Sam Devavalcante. He is a member of the DeCavalcante Family. He operates a tire business in Garfield, N. J. in which DeCavalcante is a partner.
60. JOSEPH "WHITEY" DANZO - a member of the DeCavalcante, New Jersey La Cosa Nostra Family.
61. JOE KREMER - Accountant of DeCavalcante.
62. NICK QUARINO - A member of the DeCavalcante, New Jersey La Cosa Nostra Family.
63. KINNEALY (P H) - Democratic Party Leader in Union County.
64. JUDGE ARD - A Judge in Union County, N. J.
65. SAM REIDA - A building contractor from Union County with whom DeCavalcante has had working agreements.
66. EMANUEL RIGGI - Member of DeCavalcante Family - father of John Riggi, a Caporegime of DeCavalcante. Was formerly officer of Local 394, Laborers International Union, until he was arrested by the F.B.I., Charged with antiracketeering-extortion for which he was convicted. cf. McClellan Comm-Organized Crime at Pg. 970.
67. GUS BRUGGER - Captain of Elizabeth, N.J. Police Department until appointed Director of Elizabeth by Mayor Thomas Dunn. Retired in 1968 and moved to Florida.

68. FRANK DEE - True name FRANK D'ALLESIO - member of the Carlo Gambino Family.
69. MIKE - True Full name MIKE D'ALLESIO, also known as MIKEY DEE. Member of Carlo Gambino Family - 1 of the 5 La Cosa Nostra Families in New York. Also cf. McClellan Comm-Organized Crime at Pgs. 294,652.
70. CHARLIE MAJURI - Son of Frank Majuri, Underboss of DeCavalcante. Member of DeCavalcante Family - New Jersey La Cosa Nostra Family.
71. LEO KAPLOWITZ - Union County N. J. Prosecutor. Prosecutors in New Jersey are appointed by the Governor.
72. THOMAS DUNN - Mayor of Elizabeth, N. J. Newark Evening News Edition.. 6/12/69, Pg. 1, quoted Dunn admitted knowing & meeting De-Cavalcante.
73. STEVE BERCIK - Former Mayor of Elizabeth N. J. after 8 years as Mayor, he was succeeded by Thomas Dunn.
74. MAGNOLIA - True name MICHAEL MAGNOLIA, Union County Public Works Commissioner. Republican opponent of Mayor Dunn.
75. LA CORTE - True name NICHOLAS LA CORTE, N.J. State Senator from Union County. Republican opponent of Mayor Dunn.
76. PHIL CAMORO - Cousin of DeCavalcante. Resides Red Oakes Drive, Long Branch, N. J. Former chairman of N. J. State Tenement Housing Commission.
77. ANTHONY "LITTLE PUSSY" RUSSO - Member of the Vito Genovese Family, 1 of the 5 La Cosa Nostra Families in New York. His operations principally in the New Jersey Shore area, centered around Long Branch. His brother, John "Big Pussy" Russo is close associate of Anthony "Tony Boy" Boiardo.
78. TONY BANANAS - True name ANTONIO CAPONIGRO - member of the Angelo Bruno, Philadelphia, Pa. La Cosa Nostra Family. His operations based in Newark, N. J. area.
79. DICK SPINA - True name DOMINICK SPINA, Director of Police, Newark, N. J. Police Department appointed by Mayor Hugh Addonizio. He was an Inspector in the Police Department when so appointed. He was indicted on July 25, 1968 by Essex County N. J. Grand Jury on four counts malfeasance for failure to perform duties properly - subsequently acquitted.

80. HUGHIE ADDONIZZIO - Mayor Hugh Addonizzio of Newark, N. J. elected Mayor after having served as Congressman from Essex County, N.J.
81. IRVING BERLIN - A gambler from Newark, N.J. and Essex County who bragged he was the one who coordinated the collections and assessments that the Cosa Nostra levied to finance Addonizzio's Mayoralty campaign.
82. SATZ - David Satz, former U. S. Attorney for the State of New Jersey. He resigned at end of June, 1969.
83. CORKY, True name GAETANO DOMINICK VASTOLA, member of DeCavalcante LaCosa Nostra family, transfer sponsored by Frank Cocchiaro, DeCavalcante's Capo.
84. CHIEF JOHN ELLMYER - Chief of Police of Edison Township, N. J. The roster of New Jersey State Association of Chiefs of Police for 1912-1965 lists full name as JOHN W. ELLMYER.
85. BUST-OUT MAN - One employed by operator of a crap game whose job it was to switch dice and stop a hot streak by a winning crap shooter.
86. ANGELO PICCOLELLO, also known as "PICKLES" had been under the protection of DeCavalcante until about 2 weeks before he was beaten to death in Elizabeth. He probably was not a Cosa Nostra member but more likely was an associate.
87. PETE SMITH - True full name PETER A. SMITH, employed by the state of New Jersey, Division of Professional Boards, 1100 Raymond Blvd., Newark, N. J. as Counsellor at Law and Chief Inspector. He was Special Agent of the FBI from 1949 to 1953.
88. GROVER RICHMAN - Attorney and former Attorney General of New Jersey under Governor Robert Meyner.
89. ANGELO MALANDRA - Attorney-at-Law from Southern part of New Jersey.
90. CHIEF JOHN O'MALLEY - There is no listing of a Chief of Police by this name in New Jersey, either active or retired.
91. JOE KELLY - Probably identical to Captain Joseph Kelly, New Jersey State Police who retired about 1969.
92. "GINO" FARINA - Member of La Cosa Nostra, believed to be identical to person same name, member of De Cavalcante Family.

93. ANTHONY PERRY SANTOLI, also known as JACK PANELS, A Lieutenant and long time trusted associate of Angelo "Gyp" DeCarlo. Member of the Vito Genovese Family, one of the five Cosa Nostra Families in New York. Very active in gambling, especially crap games.
94. HARRIET GOLD - Also known as HARRIET WOLFSON GOLD, MRS. DAVID GOLD, sister of Lawrence Wolfson, DeCavalcante's partner in Kenworth Corp. She is private secretary to DeCavalcante and has been having an affair with him.
95. "THIS GUY" - "DAN", True name DANIEL J. SPISSO, Director of Public Safety, East Brunswick, N. J. He was formerly a Police Officer in Plainfield, N. J., then Detective on Middlesex County Prosecutor's staff which he left to accept U.S. Government position destined for Saigon. Never went to Saigon, returning to East Brunswick job.
96. FEDS - Internal Revenue Agents
97. ROCKY, True last name INFELICE, member of LaCosa Nostra family in New York.
98. "TODDO" MARINO - True name GAETANO MARINO, Member of the Joseph Colombo LaCosa Nostra family. Cf. McClellan Commission - Organized Crime at Pgs. 308, 652.
99. JOE KUSCHENER - A Union County contractor and builder - Arco Builders, Inc., Union, N. J.; resides Elizabeth.
100. JOE WOLF, True name JOE WILF, a Union County contractor and builder - brother Harry - other principle; resides Hillside.
101. RALPH LEVEY - Partner with Joe Wilf in contracting and building - Union County.
102. MONROE MARKOWITZ - Attorney and building developer. Office located on Morris Avenue, Union, N. J.
103. BOBBY SARCONI, True name ROBERT SARCONI - former New Jersey State Senator from Essex County.
104. TONY PROVENZANO, True name ANTHONY PROVENZANO, also known as TONY PRO. Convicted head of Teamsters Local 560, now serving Federal Prison term.
105. PETE WEBER, True name PETER WEBER. Head of Operating Engineers Union. Convicted of violation of Federal Extortion laws in 1969.
106. ROBERT MURPHY - Secretary of Union Local #24 who supplied union books to DeCavalcante for payment.
107. TONY GRANDE - An associate but not a member of Cosa Nostra who is "with" (under protection of) Carlo Gambino, head of LaCosa Nostra family.

- 108. MIKE MADALIA - Probably identical to Michael Mandaglio, official of Union Local #394, Newark, N. J. He is member of Carlo Gambino La Cosa Nostra family, one of five New York City Cosa Nostra families.
- 109. SAM HALPERN - Building contractor and developer - Union County.
- 110. SAM REIDA - A Union County buidling contractor and developer.
- 111. MIKE KLEINBERG - A Union leader in Union County. Holds position in Joint Council of County wide unions.
- 112. JACK KIRSCH - Accountant of DeCavalcante, was formerly with Internal Revenue Service. Friend of Gerardo "Jerry" Catena and Carmen Battaglia.
- 113. PHIL AMARI, True name FILIPPO AMARI, also known as BIG PHIL. Former boss of the now DeCavalcante family. Returned to his birthplace Ribera, Sicily, Italy. Also cf. McClellan Commission - Organized Crime at Pgs. 894, 970.

Borrowing costs. The rise in interest rates on home mortgages is going to accelerate, predicts Chairman Thomas R. Bomar of the Federal Home Loan Bank Board. He blames the prospect on increases now being announced in rates that lending institutions pay on savings accounts. In a growing number of States, mortgage rates already are crowding up against limits of the usury laws.

Rate rollbacks. At least two commercial banks have been persuaded by the Nixon Administration to roll back their prime rate on loans to big corporations from 8 1/2 per cent to 8 1/4. They had attempted to boost that charge to 8 1/2 per cent from 8 as other banks moved up to 8 1/4.

Vanishing securities. In New York City, 16 people have been indicted on charges of conspiring to dispose of more than 18 million dollars in stolen or counterfeit securities. In Washington, D.C., a Senate investigating committee heard testimony that 5.3 billion in stolen, lost or missing securities have been recorded by just one financial service in the last three years.

PROFESSOR BLAKEY: Based on your analysis, Mr. Linehan, I wonder if you would give us an evaluation generally of the kind of information that you got from examining the documents?

MR. LINEHAN: First of all, before we were allowed to have this installation, we frankly didn't know this much activity was going on. We had heard some things about some people talking about the combination or the syndicate or something like that, but it would seem to be localized. And we discounted a lot of stuff, figuring that somebody was bragging to make Brownie points or something.

In fact, I could kick myself around the corner because I was, in the late '50's, offered a diary and address book pertaining to the 1928 organized crime meeting in Cleveland, Ohio. I examined it for a week and thought that it was a nothing and turned it back to the person. Since then, I have been calling myself all kinds of names.

PROFESSOR BLAKEY: What I am trying to raise with you, Mr. Linehan, is when you read the documents, when you read the administrative memoranda, or the transcripts, or the airtels radio-grams, how did you go about evaluating the information they contained?

MR. LINEHAN: First of all, they will not talk before the general public. They thought they were talking among themselves. And when they would say something that seemed highly improper, they were checked out by other means available. We would not have been able to do it other than through the devices, and we learned a lot of information that we didn't know before.

PROFESSOR BLAKEY: Do I understand what you are saying is that while they were being operated, the Bureau would listen to the various people and attempt to identify them, and then at-

tempt to assess the credibility of various people speaking?

MR. LINEHAN: That is right.

PROFESSOR BLAKEY: Was an effort made to verify some of the factual statements made by the people?

MR. LINEHAN: There was. For example, if we heard them say they were going to have a meeting or something of that nature, that something big was coming up, we would follow them and find out if there was a meeting, and if so how many attended. And that burned up manpower because they were very surveillance conscious, and we put three cars on each one.

PROFESSOR BLAKEY: Did you find the credibility of the subjects being overheard varied?

MR. LINEHAN: The credibility was very, very high. The only thing we had to do was to try to find out if somebody was bragging to show his stature or make himself be big. DeCavalcante was not that type.

PROFESSOR BLAKEY: For example, did you find that DeCavalcante in normal conversation was not a bragger?

MR. LINEHAN: He was not a bragger. In fact, my personal opinion is he downgraded his ability. When he was first appointed head of the family, he had about 30 soldiers. Because as you probably know, when the boss of a family dies or is removed from an area, all the appointments made by him revert to soldiers, and it is up to the new boss coming in either to reappoint them or appoint whoever he desires.

PROFESSOR BLAKEY: You said DeCavalcante was reliable. What about Angelo Bruno?

MR. LINEHAN: I believe Angelo Bruno was fairly reliable because the information we were asked to check out on him came out better than we expected. One of the capos, Tony Bananas, was flamboyant. We thought he might be less credible.

PROFESSOR BLAKEY: Could you say the same of the other people you overheard?

MR. LINEHAN: No, I believe the ones that DeCavalcante had in his county kept very much according to the protocol, apparently. The closest one to overstepping the line was his blood cousin, Bobby Basile, whose true name was Occhipinti. And the whole time he was working in New Jersey they were looking for him in New York under the name of Occhipinti.

PROFESSOR BLAKEY: So I take it your statement about the credibility of the various speakers is that some were high and some were low; and that over a period of time the Bureau made an effort to indicate that credibility.

MR. LINEHAN: That is right.

PROFESSOR BLAKEY: Would you describe for us generally the size of the DeCavalcante family as indicated by the tapes?

MR. LINEHAN: The DeCavalcante family was originally about 30 men. He had two underbosses. One was Majuri in New Jersey, and the other was LaSelva in Connecticut. DeCavalcante had an interest in Connecticut.

PROFESSOR BLAKEY: Compared to others, was the DeCavalcante family a large one or a small one?

MR. LINEHAN: A small one. It originally was 30 and he had some transfers from New York and I don't think it ever reached 50.

PROFESSOR BLAKEY: Could you give us a general assessment of the strength of the family? Was it an important and powerful family?

MR. LINEHAN: No, it was not, in the sense DeCavalcante was not himself a member of the Commission, but he stood in well with the more powerful bosses.

PROFESSOR BLAKEY: Could you give us an assessment of the size of the illegal operations? Were they large? Small? Medium?

MR. LINEHAN: Do you mean by income or expenses?

PROFESSOR BLAKEY: I really want to ask you both.

MR. LINEHAN: All right. Let's put it this way. His principal source of income was probably gambling, some shylocking, control of labor unions, and he used the labor unions so that the construction people, the builders, had an agreement that they would pay so much per room to him so that they would not be obliged to use union labor at union scale.

PROFESSOR BLAKEY: Would DeCavalcante's operations in gambling, shylocking and, say, labor corruption be large in comparison, say, to some of

the New York families?

MR. LINEHAN: Oh, it wouldn't be compared with the New York families, the money they were taking out. DeCavalcante said one time, talking to Bananas—Bananas said he kept all these people on the payroll for yard and a half, which is \$150 a week.

PROFESSOR BLAKEY: How large was the Gambino family, for example?

MR. LINEHAN: It is over 500, so far as I heard. Carlo is the most powerful one at the present time.

When Vito Genovese was the boss of bosses, his family was the largest. But after Vito died, his family lost some of theirs due to transfer—Gambino was listed as having 1,000 soldiers or members and Jerry Catena had 600. Now, Catena is of the old Genovese family. Columbo was 200. Tramonti, successor to the Tommy Luchese family, 115. And the Bonanno family is listed as 400. That's the only part I would question.

PROFESSOR BLAKEY: It is my understanding you have prepared a chart of the basic families of the Cosa Nostra.

MR. LINEHAN: That is right, sir.

PROFESSOR BLAKEY: I wonder if you would submit it for the record at this time.

MR. LINEHAN: Yes, sir. It is called, "The Cosa Nostra in 1975." It still lists Magaddino as being alive. He died a few weeks ago. The Trafficante family is listed but they are back in Florida.

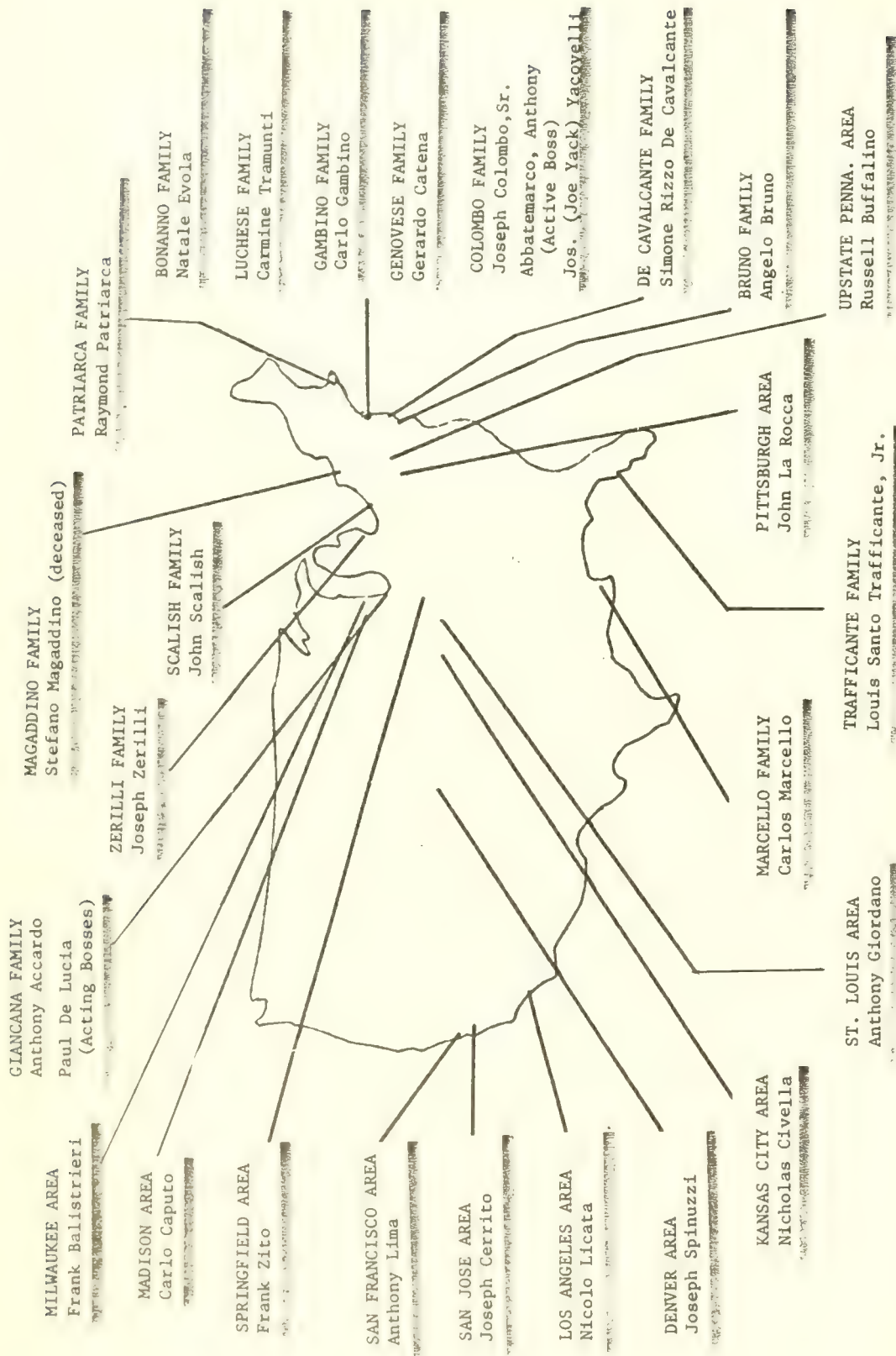
The Giancanna family—as you know, Sam Mooney Giancanna was eliminated.

PROFESSOR BLAKEY: It is my understanding that this chart was prepared from material in the public record.

MR. LINEHAN: Yes, sir, it was.

PROFESSOR BLAKEY: Without objection, it is included.

[The document referred to follows.]



LA COSA NOSTRA: 1975

PROFESSOR BLAKEY: You testified, Mr. Linehan, that the size and strength of the DeCavalcante family was small compared to the size of the other families.

MR. LINEHAN: Yes. The size was 40, and when he took over the family in 1964 he had 30. So to my knowledge he did not make any people.

PROFESSOR BLAKEY: Would it be possible, then, to infer from the tapes of the DeCavalcante family alone what the size and scope of the illegal activities of other Cosa Nostra families were?

MR. LINEHAN: If you want to project it, yes. For example, Carlo Gambino—

PROFESSOR BLAKEY: No, what I am getting at is that it has been suggested in some quarters that the picture you are painting of the DeCavalcante family is not terribly impressive, and the inference that has been drawn is that if the tapes are accurate the illegal activities of some of the other families are probably not terribly impressive either.

Would you comment on that?

MR. LINEHAN: I would not agree with that statement at all. The Gambino family has interests in a number of various ways. DeCavalcante, as I have said, was engaged in gambling but not to the same extent as some of the other families were. The Genovese family and Gambino family ran big operations. DeCavalcante ran what you'd call penny ante gambling compared to those because he allowed some of his people to take gambling debts on jobs they controlled but he was leery of gambling because he had lost money in one of the gambling games and the pay-off didn't pay off as far as he was concerned. He was closed down before he got the money back.

PROFESSOR BLAKEY: I am referring to the article by Murray Kempton that appeared in the *New York Review of Books*, September 11, 1969, entitled, "Crime Does Not Pay," in which the theme is developed that the popular literature on organized crime, indicating its size and strength and importance in the criminal area, just simply was not borne out by what was read in these tapes. When I asked you to comment whether you thought you could infer the size and strength of organized crime from the DeCavalcante tapes, whether that would be a proper inference.

MR. LINEHAN: No, I would disagree with that. The organized crime bosses, particularly those who were members of the Commission—they were appointed to the Commission because of the fact that they were powerful, had numbers of men, and they were powerful financially. I have seen it reported in the press a number of times that Gambino is worth over \$1 million.

One thing that has always been puzzling here—and I don't know if anybody knows the answer—when somebody dies, the estate very seldom goes to probate. Someone always takes over the following day as though they had been willed it before they got it.

PROFESSOR BLAKEY: Mr. Linehan, the public record indicates that the FBI also had electronic surveillance on a number of other so-called figures of organized crime in other cities. For example, there is an indication that Patriarca in New England was subjected to surveillance; Zicarelli in New Jersey was subject to surveillance; Zerilli in Detroit was subjected to surveillance; Aldoresio in Chicago was subjected to surveillance; Magaddino in Buffalo was subjected to surveillance.

During the course of your activity with reference to organized crime in New Jersey, did you have access to information that came from electronic surveillance of these others?

MR. LINEHAN: Yes, but not with all the ones you mentioned. If something came up with reference to Aldoresio that would be pertinent to us, it would be sent to us, but we were much more conversant with the ones in the New York area.

PROFESSOR BLAKEY: Let me direct your attention now not to the size or strength or nature of the activities indicated by the transcripts, but rather the nature of the organization itself, its division into bosses, underbosses, capos and soldiers.

Did you find that kind of information present in DeCavalcante tapes was confirmed by the surveillance conducted of the others?

MR. LINEHAN: Yes. They had that Borgata (family) structure principally for insulation so the authorities very seldom could reach above the capo in order to get any prosecution.

PROFESSOR BLAKEY: Mr. Linehan, at the early part of the document that you have submitted for the record, you quote the former Director of the FBI as indicating in 1966—I quote from your document now, page 2—"J. Edgar Hoover told a House of Representatives Appropriations Committee: 'The Cosa Nostra is the largest organization of the criminal underworld in this country, very closely organized and strictly disciplined.'"

Nevertheless, in 1962 the Director of the Federal Bureau of Investigation in the FBI Law Enforcement Bulletin observed: "No single individual or coalition of racketeers dominates organized crime across the nation."

How would you account for that difference in perception of the nature of organized crime from 1962 to 1965?

MR. LINEHAN: Basically it was due to ignorance and lack of any information definitely establishing that.

PROFESSOR BLAKEY: Is it your testimony that the FBI did not know there was a Cosa Nostra in 1962, or at least it was not generally known within the Bureau that there was a Cosa Nostra in 1962 when the Director made this statement?

MR. LINEHAN: In 1962 for the first time we learned of La Cosa Nostra, and that was through the installation of the device you referred to previously in the Bruno family. And that is set forth in this report. I think it is set forth on page 7, Mr. Blakey. "There is an organization called Cosa Nostra."

But I'd like to point out when we first heard it, we thought it was La C-a-u-s-a Nostra because the one talking had an accent which sounded more like a broad A. And in the evaluation at that time, we were trying to find out just what it was. A lot of the writers subsequently have said we knew nothing about this until Valachi testified. Valachi just said there was no Mafia.

PROFESSOR BLAKEY: It has been suggested in an article by Tom Wicker in the *New York Times Magazine*, December 1969, that the change in position by the former Director was related to a desire to—and I am paraphrasing—have a substitute Communist menace, that is, a Mafia menace that he could take up to Congress and obtain high appropriations. I think that is a fair characterization.

Based on your experience in the Bureau, was there any truth to that?

MR. LINEHAN: I would say not. At that time we were busy enough on regular crime, and when we started on organized crime we had very few agents until we started showing productiveness.

But these transcripts and these other devices that have been made public should clearly indicate that these people were talking about what they were planning and what they were going to do, and the amount of money they were taking in illegally throughout the country.

Even if we discount it by saying they are bragging about their money, we cannot go along and say this was a specter set up by J. Edgar Hoover. Because these people were in business long before we knew about it. And they were organized.

Up until that particular time it was my impression, and probably the impression of some of the others working for them, that we had local groups, and it was a friendship basis and not an organized basis.

PROFESSOR BLAKEY: Mr. Linehan, Dwight C. Smith in his recent book, *The Mafia Mystique*, discusses this question of where the notions of "Mafia" and "Cosa Nostra" come from and describes their history and development. I am now quoting from page 296.

"The difference in 1960 came from a combination of a series of intercepted conversations from DeCavalcante's office and a theoretical formulation of La Cosa Nostra the President's Crime Commission introduced earlier. They gave a substance to the Mafia that had been missing earlier. But how reliable was the evidence? Under close examination, it offers little more than earlier probes."

[Material omitted.]

"When examined, however, their revelations were often ambiguous."

[Material omitted.]

"Boasting, lies, and manipulative statements for effect all stemmed from the same base as did statements of the facts and truth. In the interpretation of them, summaries or summaries of summaries, obviously depending on third-party interpretations, had to be based on what the primary listener expected to hear."

I take it the thrust of Mr. Smith's point was that the FBI, far from learning something from these devices, was confirming a theory that it already had.

Does your examination of these materials indicate that was true?

MR. LINEHAN: It indicates that that statement is completely false, without any basis whatsoever.

PROFESSOR BLAKEY: Directing your attention now to the airtels and logs before you of 2-11-62—

MR. LINEHAN: Yes, sir.

PROFESSOR BLAKEY: —would you point out for the Commission and explain for us the material in reference to "Causa Nostra" and "Cosa Nostra"?

MR. LINEHAN: The conversation on that date took place between Bruno, Ignatius Denaro or Gnatz, and DeCavalcante, who was described as a gambler. The bulk of the conversation was in English. At times, the conversation was carried on in a highly excitable fashion, resulting in the inability of transcribers to determine exactly what was said. It should be noted that both Angelo Bruno and DeCavalcante spoke primarily in English.

PROFESSOR BLAKEY: The part I am referring to, I believe, Mr. Linehan, is marked with a paper clip, and I am referring to the administrative memo.

MR. LINEHAN: The administrative memo?

PROFESSOR BLAKEY: Will you turn to the one on the Cosa Nostra and we will just read that one passage.

[Discussion off the record.]

PROFESSOR BLAKEY: Directing your attention back, Mr. Linehan, to the administrative memorandum dealing with the conversation of 2-11-62.

MR. LINEHAN: Right.

PROFESSOR BLAKEY: Would you read for the reporter the material dealing with Special Agent Hagerty's interpretation of the conversation?

MR. LINEHAN: He, in reviewing this tape and the transcript, says:

"Unknown phraseology is utilized by members of the Philadelphia Italian family in the above-mentioned matters, namely:

"1. Use of the term C-a-u-s-a Nostra, which refers to matters of importance to the family."

PROFESSOR BLAKEY: Let's stop right there. This is as of 2-11-62?

MR. LINEHAN: That's 2-11-62.

PROFESSOR BLAKEY: Is that interpretation of the tape correct?

MR. LINEHAN: It is correct except for the spelling of the one word.

PROFESSOR BLAKEY: No, what I am referring to is Special Agent Hagerty there identifies matters relating to the family as Causa Nostra.

MR. LINEHAN: That is correct. It is correct.

PROFESSOR BLAKEY: So his interpretation is correct?

MR. LINEHAN: His interpretation was correct at that time. The Cosa Nostra was of concern to the members of the family.

PROFESSOR BLAKEY: Was it also the name, Cosa Nostra?

MR. LINEHAN: No, it was, but his interpretation seems to indicate it only as the family. He refers only to "the family," not referring to all the families, but in a later interpretation they referred to each one of the families, so it became La Cosa Nostra, C-o-s-a.

Second was the use of the word "amico nostro," as a term reflecting membership in the family or the organization.

That interpretation was entirely correct and has been supported and developed further through the years.

Third, the use of the word "udienza." This he interpreted as being an audience, and was more or less a discussion of a soldier in the family with his immediate boss, so it is an audience in that particular sense.

He explains it as, "Amico nostro is discussing the matter."

He then says that Angelo Bruno was the caporegima in the Philadelphia area.

PROFESSOR BLAKEY: Is that a correct interpretation?

MR. LINEHAN: It is not a correct interpretation. Angelo Bruno was the boss of the family, and in the structure of the family the boss is separated from the caporegima by the underboss. So the boss can give a suggestion to the underboss. He, in turn,

gives it to the caporegima who will pass it on to the soldier.

PROFESSOR BLAKEY: If I understand you correctly, Mr. Linehan, your analysis of these materials indicates the Bureau agent's interpretations were in error?

MR. LINEHAN: That is right.

PROFESSOR BLAKEY: That as you listened over a longer period of time, your understanding, far from showing, as Mr. Smith indicates in his book—you didn't go in to verify a theory. You went in and looked on a case-by-case basis and came up initially with some erroneous theories, and only after a considerable period of time did you only carefully identify what the materials the materials really were.

MR. LINEHAN: That is correct. We had to change our spelling and structure of our set-up.

PROFESSOR BLAKEY: You previously indicated, Mr. Linehan, that portions of these tapes were originally spoken in a foreign language?

MR. LINEHAN: That is right.

PROFESSOR BLAKEY: And had to be translated.

MR. LINEHAN: They were translated by either Italian-speaking agents or individuals who took Italian courses.

We had the situation sometimes in which the Italian-speaking agent might not understand the Sicilian dialect used, and he'd have to ask a person familiar with Sicilian.

PROFESSOR BLAKEY: Did it ever happen that no Italian-speaking agent was listening and the Italian parts were lost?

MR. LINEHAN: Yes. This is the human element. Somebody would say, "They spoke in a foreign language. Couldn't read it. No value."

They'd dismiss it because they couldn't understand it and would not appeal for help.

PROFESSOR BLAKEY: Our record already indicates a study was conducted of 12 or 13 of these devices and some were indicated to have been not productive.

Would they perhaps have been not productive in part because of this human factor you indicated?

MR. LINEHAN: I would say quite likely, and also possibly the possibility some people like to work 8:00 to 5:00, or something like that.

PROFESSOR BLAKEY: Let me ask you one final question.

We have testimony in the record by the former Attorney General Ramsey Clark that this surveillance obtained no convictions, and therefore he felt that it was unproductive. He also indicated that he felt it was unproductive in the sense of obtaining criminal intelligence.

I wonder if your study and your evaluation of the documents would indicate that they were unproductive from the point of view of criminal intelligence?

MR. LINEHAN: From the point of view of criminal intelligence they were invaluable because they gave us an indication as to what was going on not only in our area but in other areas. We were the only ones to have any information about the skims, for example, the fact that they were taking money off the top in Las Vegas. That was done in the early 1960's. And we got in New Jersey as a result of this

device—not only this device but other devices.

PROFESSOR BLAKEY: Thank you, Mr. Linehan.

Without objection, I would like to enter in the record at this time selected excerpts from the public record indicating the Department of Justice's policy on wiretapping and electronic surveillance from 1928 to 1968, just prior to the statute, and note that it indicates the general legal theory under which this surveillance was conducted.

[The document referred to follows.]

SELECTED DOCUMENTS FROM THE
PUBLIC RECORD

In 1928, after *Olmstead v. United States*, 277 U.S. 438 (1928), the legal status of wiretapping was easily summed up—it was neither unconstitutional nor a federal crime, and evidence obtained by it was admissible in federal courts. See, e.g., *Foley v. United States*, 64 F.2d 1 (5th Cir.), *cert. denied*, 289 U.S. 762 (1933). This position was, however, reversed but ten years later in the *Nardone* decisions, 302 U.S. 379 (1937) and 308 U.S. 338 (1938), in which the Supreme Court, despite legislative history indicating that the "bill . . . does not change existing law," 78 CONG. REC. 10313 (1934), construed Section 605 of the Federal Communications Act of 1934, 48 Stat. 1103 (1934), 47 U.S.C. § 605 (1957) to make wiretapping a federal crime, and its fruit inadmissible in federal courts. It was in this setting that then Attorney General Robert H. Jackson, on March 13, 1940, issued the following statement:

Upon the recommendation of Director J. Edgar Hoover of the Federal Bureau of Investigation, Attorney General Robert H. Jackson today issued the following order:

"As of this date the provision of the manual governing the operations of the Federal Bureau of Investigation, which was adopted in 1931 on order of the Attorney General, and which reads as follows, is superseded:

"Wire tapping: Telephone or telegraph wires shall not be tapped unless prior authorization of the Director of the Bureau has been secured."

In its place and stead there is hereby reinstated the provision of the manual which prevailed until 1931:

"Unethical tactics: Wire tapping, entrapment, or the use of any other improper, illegal, or unethical tactics in procuring information in connection with investigating activity will not be tolerated by the Bureau."

There will further issue to all United States attorneys and attorneys of the Department of Justice orders directing that no case originating in or investigated by any other department of the Government be presented to grand jury or otherwise prosecuted in which it appears that the case has been developed in whole or in part as the result of wire tapping after April 1, 1940. Any case so developed shall be called to the attention of the Assistant Attorney General in charge of the Division and shall not be presented except upon special direction of the Attorney General.

This action is required in order that the rules governing the Federal Bureau of Investigation shall conform to the decisions of the Supreme Court in recent cases, which have held interception and divulgence of any wire communication to be forbidden by the terms of the Communications Act of 1934. These decisions have in effect overruled the contentions of the Department that it might use wire tapping in its crime-suppression efforts.

Charges of violation of several Federal laws, such as the income-tax laws, narcotic law, mail-fraud statute, and alcohol-tax law, are not investigated by the Federal Bureau of Investigation but by other departments of the Government. These agencies are not bound by this rule of the Attorney General. But all their cases are presented to grand juries and courts by Department of Justice attorneys. Cases, wherever originating, must, under this rule, be free of illegality on the part of the Government if they are to be presented to courts under the sponsorship of the Department of Justice. From the time of its reorganization (in 1924) under Attorney General Stone until 1931 the practice of wire tapping was not authorized in the Bureau of Investigation.

In 1931 the Department of Justice had two investigative forces, the Federal Bureau of Investigation, in which wire tapping was prohibited, and the Prohibition Enforcement Bureau, in which wire tapping was resorted to. In 1931 Attorney General Mitchell was confronted with the inconsistency of the two practices and stated to a House Appropriations Committee as follows:

"The present condition in the Department cannot continue. We cannot have one bureau in which wire tapping is allowed and another in which it is prohibited. The same regulations must apply to all . . . I think I should give a direction applicable to all bureaus and divisions in the Department that no tapping of wires should be permitted to any agent of the Department without the personal direction of the chief of the bureau involved after consultation with the Assistant Attorney General in charge of the case. Something, of course, can be said in favor of permitting the tapping of wires when efforts are being made to detect the perpetrators of heinous offenses or to apprehend and bring to punishment desperate gangs of criminals. In such cases the criminals are usually equipped with all modern scientific inventions such as the radio, the telephone, and the automobile, and the Government is at a considerable disadvantage in any event in dealing with them."

Thereafter the rules were amended to permit wire tapping by the Federal Bureau of Investigation in the discretion of the Director.

I am informed by the Director that this authority has been very little used and only in cases of extreme importance, that without the use of wire tapping several kidnapping cases would not have been solved; and that wire tapping has never been used in minor cases nor on Members of Congress, or officials, or any citizen except where charge of a grave crime had been lodged against him.

In view of the widespread charges of indiscriminate wire tapping, it is only fair to Mr. Hoover to state that the records of this Department show that on two occasions he has advised strongly against extension of wire tapping. In March 1939 he advised this Department to oppose a bill pending in Congress to legalize wire tapping, and stated his view as follows:

"While I concede that the telephone tap is from time to time of limited value in the criminal investigative field, I frankly and sincerely believe that if a statute of this kind were enacted the abuses arising therefrom would far outweigh the value which might accrue to law enforcement as a whole."

Upon another occasion he advised this Department against trying to sustain in the Supreme Court the practice of wire tapping.

Notwithstanding it will handicap the Federal Bureau of Investigation in solving some extremely serious cases, it is believed by the Attorney General and the Director of the Bureau that the discredit and suspicion of the law-enforcing branch which arises from the occasional use of wire tapping more than offsets the good which is likely to come to it. We have therefore completely abandoned the practice as to the Department of Justice.

In a limited class of cases, such as kidnaping, extortion, and racketeering, where the telephone is the usual means of conveying threats and information, it is the opinion of the present Attorney General, as it was of Attorney General Mitchell, that wire tapping should be authorized under some appropriate safeguard. Under the existing state of law and decisions, this cannot be done unless Congress sees fit to modify the existing statutes.

(86 CONG. REC. APP. 1471-72 (1940))

Nevertheless, the Jackson order was short lived. President Franklin D. Roosevelt, in a confidential memorandum, dated May 21, 1940, instructed the Attorney General in these terms:

I have agreed with the broad purpose of the Supreme Court decision relating to wiretapping in investigations. The Court is undoubtedly sound in regard to the use of evidence secured over tapped wires in the prosecution of citizens in criminal cases and is also right in its opinion that under ordinary and normal circumstances wiretapping by Government agents should not be carried on for the excellent reason that it is almost bound to lead to abuse of civil rights.

However, I am convinced that the Supreme Court never intended any dictum in the particular case which it decided to apply to grave matters involving the defense of the nation.

It is, of course, well known that certain other nations have been engaged in the organization of propaganda of so-called "fifth columns" in other countries and in preparation for sabotage as well as actual sabotage.

It is too late to do anything about it after sabotage, assassination and 'fifth column' activities are completed.

You are, therefore, authorized and directed in such cases as you may approve, after investigation of the need in each case, to authorize the necessary investigating agents that they are at liberty to secure information by listening devices directed to the conversation or other communications of persons suspected of subversive activities against the Government of the United States, including suspected spies. You are requested furthermore to limit these investigations so conducted to a minimum and to limit them insofar as possible to aliens.

(N. Y. Times, June 19, 1967, p. 22, col. 2)

In March 1941, in a letter to Congress urging adoption of wiretapping legislation, Jackson then announced that the "only offense under the present law [Section 605] is to intercept any communication and divulge or publish . . . [it]. Any person, with no risk of penalty, may tap telephone wires . . . and act upon what he hears or make any use of it that does not involve divulging or publication." *To Amend the Wiretapping Laws, Hearings before Subcommittee No. 1 of the House Committee on the Judiciary on H.R. 2266 and H.R. 3099*, 77 Cong., 1st Sess. 18 (1941).

The Roosevelt memorandum, and Jackson's revised interpretation of Section 605, remained the foundation of federal practice until Tom C. Clark became Attorney General in 1945. Mr. Clark sought the authority of President Harry S. Truman to extend the power of interception in these terms:

"Under date of May 21, 1940, President Franklin D. Roosevelt, in a memorandum, addressed to Attorney General Jackson, said:

" 'You are, therefore, authorized and directed in such cases as you may approve, after investigation of the need in each case, to authorize the necessary investigating agents that they are at liberty to secure information by listening devices directed to the conversations or other communications of persons suspected of subversive activities against the Government of the United States, including suspected spies.' "

"This directive was followed by Attorneys General Jackson and Biddle, and is being followed currently in this department. I consider it appropriate, however, to bring the subject to your attention at this time.

"It seems to me that in the present troubled period in international affairs, accompanied as it is by an increase in subversive activity here at home, it is as necessary as it was in 1940 to take the investigative measures referred to in President Roosevelt's memorandum. At the same time, the country is threatened by a very substantial increase in crime. While I am reluctant to suggest any use whatever of these special investigative measures in domestic cases, it seems to me imperative to use them in cases vitally affecting the domestic security, or where human life is in jeopardy.

"As so modified, I believe the outstanding directive should be continued in force. If you concur in this policy, I should appreciate it if you would so indicate at the foot of this letter.

"In my opinion, the measures proposed are within the authority of law, and I have in the files of the department materials indicating to me that my two recent predecessors as Attorney General would concur in this view."

(N.Y. Times, June 19, 1967, p. 22, col. 2)

Mr. Truman added his "I concur" on July 17, 1947. This extension, however, was not made public. In a press release, dated March 31, 1949, Attorney General Clark stated: "There has been no new policy or procedure since the initial policy was stated by President Roosevelt, and this has continued to be the department's policy whenever the security of the nation is involved." N. Y. Times, June 19, 1967, p. 22, col. 7.

The Supreme Court decided three cases during this period and afterward dealing with electronic surveillance techniques other than wiretapping. In *Goldman v. United States*, 316 U.S. 129 (1942), the Court held that microphone surveillance accomplished without a physical trespass into a constitutionally protected area was not unconstitutional. In *Irvine v. California*, 347 U.S. 128 (1954), and *Silverman v. United States*, 365 U.S. 505 (1961), the Court decided that such surveillance accomplished by such a trespass violated the Fourth Amendment. At this time, the Department of Justice had no publicly stated policy in this area. Its policy, at least in one area, was as follows:

May 20, 1954 "CONFIDENTIAL"

To: Director
From: The Attorney General
Subj: Microphone Surveillance

The recent decision of the Supreme Court entitled *Irvine v. Calif.*, 347 US 128, denouncing the use of microphone surveillances by city police in a gambling case makes appropriate a reappraisal of the use which may be made in the future by the Federal Bureau of Investigation of microphone surveillance in connection with matters relating to the internal security of the country.

It is clear that in some instances the use of microphone surveillance is the only possible way of uncovering the activities of espionage agents, possible saboteurs, and subversive persons. In such instances I am of the opinion that the national interest requires [that] microphone surveillance be utilized by the Federal Bureau of Investigation. This use need not be limited to the development of evidence for prosecution. The FBI has an intelligence function in connection with internal security matters equally as important as the duty of developing evidence

for presentation to the courts and the national security requires that the FBI be able to use microphone surveillance for the proper discharge of both of such functions. The Department of Justice approves the use of microphone surveillance by the FBI under these circumstances and for these purposes. I do not consider that the decision of the Supreme Court in *Irvine v. California* requires a different course. That case is really distinguishable on its facts. The language of the Court, however, indicates certain uses of microphones which it would be well to avoid, if possible, even in internal security investigations. It is quite clear that in the *Irvine* case the Justices of the Supreme Court were outraged by what they regarded as the indecency of installing a microphone in a bedroom. They denounced the utilization of such methods of investigation in a gambling case as shocking. The Court's action is a clear indication of the need for discretion and intelligent restraint in the use of microphones by the FBI in all cases, including internal security matters. Obviously, the installation of a microphone in a bedroom or in some comparably intimate location should be avoided wherever possible. It may appear, however, that if important intelligence or evidence relating to matters connected with the national security can only be obtained by the installation of a microphone in such a location and under such circumstances the installation is proper and is not prohibited by the Supreme Court's decision in the *Irvine* case.

Previous interpretations which have been furnished to you as to what may constitute a trespass in the installation of microphones, suggest that the views expressed have been tentative in nature and have attempted to predict the course which courts would follow rather than reflect the present state of the law. It is realized that not infrequently the question of trespass arises in connection with the installation of a microphone. The question of whether a trespass is actually involved and the second question of the effect of such a trespass upon the admissibility in Court of the evidence thus obtained, must necessarily be resolved according to the circumstances of each case. The Department in resolving the problems which may arise in connection with the use of microphone surveillance will review the circumstances of each case in the light of the practical necessities of investigation and of the national interest which must be protected. It is my opinion that the Department should adopt that interpretation which will permit microphone coverage by the FBI in a manner most conducive to our national interest. I recognize that for the FBI to fulfill its important intelligence function, considerations of internal security and the national safety are paramount, and therefore, may compel the unrestricted use of the technique in the national interest.

(Investigating the FBI [edited by
D. Walters and S. Gillers] pp.
297-399 [1973])

Nevertheless, this position did not become public until the Supreme Court requested such a statement in *Black v. United States*, No. 1029, Oct. Term 1965, a case in which the Solicitor General acknowledged that unlawful microphone surveillance had been employed. Following is the statement of the Department's policy

2. No specific statute or executive order was relied upon in the installation of the listening device in question. Under 5 U.S.C. 300, the Attorney General has the authority to appoint officials for the detection and prosecution of crimes against the United States. In carrying out this responsibility, Attorneys General have delegated to the Director of the Federal Bureau of Investigation the duty to gather intelligence, to investigate violations of federal laws, and to collect evidence in cases in which the United States is or may be a party. See 28 C.F.R. § 0.85 (1966 rev.).

An exception to the general delegation of authority has been prescribed, since 1940, for the interception of wire communications, which (in addition to being limited to matters involving national security or danger to human life) has required the specific authorization of the Attorney General in each instance. No similar procedure existed until 1965 with respect to the use of devices such as those involved in the instant case, although records of oral and written communications within the Department of Justice reflect concern by Attorneys General and the Director of the Federal Bureau of Investigation that the use of listening devices by agents of the government should be confined to a strictly limited category of situations. Under Departmental practice in effect for a period of years prior to 1963, and continuing into 1965, the Director of the Federal Bureau of Investigation was given authority to approve the installation of devices such as that in question for intelligence (and not evidentiary) purposes when required in the interest of internal security or national safety, including organized crime, kidnappings and matters wherein human life might be at stake. Acting on the basis of the aforementioned Departmental authorization, the Director approved installation of the device involved in the instant case.

Present Departmental practice, adopted in July 1965 in conformity with the policies declared by the President on June 30, 1965, for the entire federal establishment, prohibits the use of such listening devices (as well as the interception of telephone and other wire communications) in all instances other than those involving the collection of intelligence affecting the national security. The specific authorization of the Attorney General must be obtained in each instance when this exception is invoked.

(Black v. United States, No. 1029, Oct. Term 1965, Supplemental Memorandum for the United States, pp. 2-4.)

The policy of the Department was further explained to the Court in *Schipani v. United States*, No. 504, Oct. Term 1966, in these terms: (footnotes omitted)

4. In view of this Court's supervisory role in the federal judicial system, the Department of Justice believes it appropriate to appraise the Court of its policy in regard to electronic surveillance of the kind here involved. Present governmental practice, adopted in July 1965 in conformity with the policy declared by the President on June 30, 1965, for the entire federal establishment, prohibits such electronic surveillance in all instances except those involving the collection of intelligence with respect to matters affecting national security. Such intelligence data will not be made available for prosecutorial purposes, and the specific authorization of the Attorney Gen-

eral must be obtained in each instance when the national security exception is sought to be invoked.³

Recognizing its obligation not to use evidence obtained in violation of a defendant's protected rights in any criminal prosecution, the Department has initiated a program to discover prior instances in which this may have occurred. An extensive review is presently being conducted in order to determine the instances in which there might have been monitoring affecting a case which has been brought to trial.⁴ Reports of the results of this continuing review are being sent to the Acting Attorney General. Similarly, a careful review of pending and prospective prosecutions is being conducted by the Department for the purpose of determining what other cases might fall within this category. This will necessarily be a time-consuming process but will be diligently pursued to completion. The government will promptly notify the appropriate court when any material discovery is made.⁵

(Schipani v. United States, No. 504 Oct. Term 1966,
Supplemental Memorandum for the United States, pp. 4-5.)

Finally, on June 16, 1967, Attorney General Ramsey Clark issued the following policy statement:

Office of the Attorney General
Washington, D C , June 16, 1967

Memorandum to the Heads of Executive Departments and Agencies
Re: Wiretapping and Electronic Eavesdropping

It is essential that all agencies having any responsibility for law enforcement take steps to make certain that electronic and related devices designed to intercept, overhear or record private verbal communications be subject to tight administrative control to assure that they will not be used in a manner which is illegal and that even legal use of such devices will be strictly controlled. In order further to assist you to achieve these ends, the following rules have been formulated.

I. Prohibition against Use of Mechanical or Electronic Devices to Intercept, Overhear or Record Conversations

A. Prohibition against Interception of Telephone Conversations.

1. Section 605 of the Communications Act (Title 47, U.S.C. § 605) prohibits the interception and divulgence or use of telephone communications and is applicable to federal law enforcement agents.

³ A memorandum of the Acting Attorney General of November 3, 1966, addressed to all United States Attorneys, summarizes the Department's policy in this regard as follows:

This Department must never proceed with any investigation or case which includes evidence illegally obtained or the fruits of that evidence. No investigation or case of that character shall go forward until such evidence and all of its fruits have been purged and we are in a position to assure ourselves and the court that there is no taint or unfairness. We must, also, scrupulously avoid any situation in which an intrusion into a confidential relationship would deny a fair hearing to a defendant or person under investigation.

⁴ As the instant case illustrates, problems in this regard may still arise in cases in which some investigation was conducted prior to July 1965.

⁵ Footnote omitted.

2. Interception by federal personnel of telephone conversations, by any mechanical or electronic device, unless with the consent of one of the parties to the conversation, is prohibited by Presidential directive, and this prohibition applies whether or not the information which may be acquired through interception is intended to be used in any way or to be subsequently divulged outside the agency involved. Any question as to whether the use of a particular device can be said to involve a prohibited interception of a telephone conversation should be referred to the Department of Justice.

3. To further assure protection of the privacy of telephone conversations, each agency shall adopt rules governing the interception by its personnel of telephone conversations under circumstances where a party to the conversation has consented. Such rules shall, where appropriate, provide for the advance approval by the agency head of such interception.

B. Prohibition against Overhearing and Recording of Non-telephone Conversations are discussed in paragraphs 1-3 below. These principles are consistent with the recent decision of the Supreme Court in *Berger v. New York*, 35 Law Week 4649, decided June 12, 1967.

1. Eavesdropping in any form which is accomplished by means of a trespass into a constitutionally protected area is a violation of the Fourth Amendment. The penetration by inches into a party wall by the spike microphone has been held to involve a trespass. *Silverman v. United States*, 365 U.S. 505 (1961). And, although the question has not been squarely decided, there is support for the view that any electronic eavesdropping on conversations in constitutionally protected areas is a violation of the Fourth Amendment even if such surveillance is accomplished without physical trespass or entry. Homes, private offices, hotel rooms and automobiles are clear examples of constitutionally protected areas, but other locations may also be held within the scope of constitutional protection depending upon the particular circumstances.

2. Even where no invasion of a constitutionally protected area has occurred, surreptitious electronic surveillance involving an intrusion into a privileged relationship, such as that of attorney-client, may violate rights entitled to protection under constitutional provisions other than the Fourth Amendment, including the First, Fifth and Sixth Amendments.

3. Under presently controlling court decisions, however, certain uses of electronic devices are legal. See, for example, the decisions in *Lopez v. United States*, 373 U.S. 427 (1963) and in *Osborn v. United States*, 385 U.S. 323 (1966), where the use of recording devices was held to be legitimate if the consent of a party to the conversation had been obtained. Moreover, the use of mechanical or electronic equipment to record statements intended to be disseminated to the public generally, public speeches for example, is clearly not illegal and is not subject to the rules formulated in this memorandum.

4. In the light of the immediately foregoing discussion in paragraphs 1-3, any use of mechanical or electronic devices by federal personnel to overhear or record non-telephone conversations involving a violation of the Constitution or a statute is prohibited.

5. In order further to assure protection of the right of privacy, to resolve questions which may arise under paragraph 4 and strictly to limit legal electronic surveillance, agencies shall, except as provided in paragraph II. 2 below, obtain advance written approval from the Attorney General for any use of mechanical or electronic devices to overhear or record non-telephone conversations without the consent of all of the parties to such conversations.

II. Controls Over the Use of Mechanical or Electronic Equipment

1. A request for advance approval from the Attorney General pursuant to paragraph I.B.5. hereof for the use of mechanical or electronic devices to overhear or record non-telephone conversations shall be made to the Attorney General in writing by the head of the requesting investigative agency and shall contain the following information: (a) the reason for such proposed use; (b) the type of equipment to be used; (c) the name of the person involved; (d) the proposed location of the equipment, (e) the duration of proposed use; and (f) the manner or method of installation.

2. If, in the judgment of the head of the investigative agency involved, the emergency needs of an investigation preclude obtaining such advance approval from the Attorney General, he may, without having obtained such approval, authorize the use of mechanical or electronic devices to overhear or record non-telephone conversations without the consent of all of the parties thereto. In any such circumstances, however, the head of the investigative agency shall, within twenty-four hours after authorizing such use, provide the Attorney General in writing with the information referred to in paragraph II. 1, above, and with an explanation of the circumstances upon which he based the judgment that the emergency needs of the investigation precluded him from obtaining such written advance authority.

3. In connection with the use of mechanical or electronic devices authorized above, the responsible agent shall, where technically feasible, record the conversations overheard by means of a tape or similar permanent record. The responsible agent shall preserve the tape or other permanent record of the conversations. He shall also submit to the investigative agency a written report setting forth the actual use or uses made of each mechanical or electronic device in connection with the authorization. Such report, the tapes or other permanent records of conversations, and any logs, transcripts, summaries or memoranda and similar material which may have been prepared shall be treated as agency records, but shall be specially classified, filed and safeguarded and shall not, nor shall information contained in such material be made available to agency personnel or others except when essential to government operations. A record shall be made and retained concerning each person to whom such information or material has been made available.

4. The head of each investigative agency should be responsible for limiting the procurement of devices primarily designed to be used surreptitiously to overhear or record conversations to the minimum necessary for use consistent with the rules formulated herein. To the extent possible, all mechanical or electronic devices used in intercepting, overhearing or recording conversations shall be stored in a limited number of locations to insure effective administrative control.

5. The agency shall maintain an inventory of all such equipment at the place where it is stored, including a record of the date that the equipment was assigned to an agent and the date the equipment was returned. Copies of these records should also be maintained at agency headquarters, together with a written report of the responsible agent referred to in paragraph II. 3 heretof. All agency records should be maintained for a period of six years.

6. The head of each investigative agency shall submit to the Attorney General on July 1st of each year a report of all uses of mechanical or electronic equipment by such agency during the previous year in accordance with the rules formulated in this memorandum, containing with respect to each use the information required by paragraph II. 1, above, and a brief description of the results obtained. The report shall also include a complete inventory of the devices referred to in paragraph II. 4, above, in the possession of the agency.

7. The functions to be exercised by the head of an investigative agency in accordance with this memorandum may be delegated by him to another officer of his agency.

III. National Security

The foregoing rules have been formulated with respect to all agency investigations other than investigations directly related to the protection of the national security. Special problems arising with respect to the use of devices of the type referred to herein in national security investigations shall continue to be taken up directly with the Attorney General in the light of existing stringent restrictions.

Ramsey Clark,
Attorney General.

(Controlling Crime Through More Effective Law Enforcement, *Hearings before the Subcommittee on Criminal Law and Procedure, Committee on the Judiciary, United States Senate, 90th Cong., 1st Sess. 922-24 (1967)*)

PROFESSOR BLAKEY: Mr. Linehan, I thank you for coming up and appearing before the Commission and for making available to it the study you did for the Subcommittee on Criminal Laws and Procedures while I was Chief Counsel. It was of enormous help to the Subcommittee at that time in analyzing the nature of organized crime, and I am sure it will be of enormous assistance to the readers of this Commission's record in judging what organized crime is and how it operates.

Thank you very much.

PROFESSOR BLAKEY: We will take a short recess now, and when we return I will pass the gavel to my kind friend on my right, Dr. Alan Westin, and indicate my regret that I have to leave to catch an airplane. I'm sorry I can't stay for the rest of the testimony.

[Whereupon, a short recess was taken.]

MR. WESTIN: The Commission will now resume. We continue with testimony regarding the monitoring of telephones, hearing from three witnesses who have had actual experience with the investigation of so-called blue box cases.

We have Mr. Neil Beller, Division Attorney, Central Telephone Company of Nevada; Mr. Michael Simon, Special Agent, Federal Bureau of Investigation, Las Vegas; and Karl Berolzheimer of the Central Telephone and Utilities Corporation.

You gentlemen have already been sworn.

Counsel will proceed to question.

**TESTIMONY OF NEIL BELLER,
DIVISION ATTORNEY, CENTRAL
TELEPHONE COMPANY OF NEVADA;
MICHAEL SIMON, SPECIAL AGENT,
FEDERAL BUREAU OF
INVESTIGATION, LAS VEGAS; and
KARL BEROLZHEIMER, CENTRAL
TELEPHONE AND UTILITIES
CORPORATION COUNSEL**

MR. WESTIN: Just for the record, I wonder if we could ask each of you to state your names and position?

MR. BEROLZHEIMER: Karl Berolzheimer. I am a member of Ross, Hardies, O'Keefe, Babcock & Parsons, attorneys in Chicago, Illinois. My home address is 414 Ashland Avenue, Evanston, Illinois.

MR. FELDMAN: Mr. Berolzheimer, I understand you have a prepared statement which you presented to the Commission.

MR. BEROLZHEIMER: I have a very brief statement, a copy of which I gave to you earlier today.

MR. FELDMAN: We will enter it into the record in that form, considering the shortness of time.

MR. BEROLZHEIMER: I would, if I might, just make two comments about it.

The purpose of preparing the statement was to essentially state the policy position of Central Telephone and Utilities Corporation, which is the parent company of Central Telephone Company by whom Mr. Beller is employed, with respect to these issues. And there are two points I'd simply like to make.

The first is with respect to Section 1344 which Mr. Caming has referred to in his testimony. It is our position that we believe such a statute would be useful and should be adopted.

Secondly, I simply want to point out, and have in my prepared statement, that although the Central Telephone Company experience indicated that convictions for violation of Section 1343 were obtained without voice recording, that experience does not necessarily indicate that voice recording is not essential, and accordingly we would agree again with Mr. Caming that under some circumstances voice recording could be essential to obtain a conviction.

MR. WESTIN: I just feel it is fair and proper for me to say that even though there is only one Commission member and members of the staff left, the Commission members will read the record, and you can be sure what you say and comments you give in answer to the questions will have the full attention of the record, and even though it looks as though you are playing to a bare house, the fact is you are speaking to the whole audience.

MR. FELDMAN: Mr. Beller.

MR. BELLER: Neil Beller, 125 Las Vegas Boulevard South, attorney.

MR. FELDMAN: Your occupation?

MR. BELLER: Attorney.

MR. SIMON: Agent Simon. Michael G. Simon, Special Agent of the FBI, assigned to the Las Vegas office.

MR. FELDMAN: Mr. Beller, have you been assigned to the investigation of a number of electronic toll fraud cases?

MR. BELLER: Yes, I was.

MR. FELDMAN: Would you tell us how many investigations you were involved in and the approximate period of time?

MR. BELLER: From April 22, 1973, through October 15 of 1973, we gave approximately 32 numbers to the FBI.

MR. FELDMAN: When you say you gave so many numbers, what does that indicate?

MR. BELLER: We had reason to believe these individuals were using some sort of device on their telephones.

MR. FELDMAN: Would you state on what basis you had that belief?

MR. BELLER: We have a computer printout, a copy of which I have here, which was for selected

numbers. These are toll-free network numbers, and by studying these numbers and ascertaining where the called number was, we had reason to believe that the person was using a foreign device.

The reason for that is that some of the numbers that were called were numbers, for example, to New York information, or the information office at TWA. And it is not logical for a person to talk to TWA for 20 minutes or a half-hour.

Based upon that, we then would put either a brush recorder or at a later date we subsequently acquired another device, which emitted a tape such as this. And from that we were able to ascertain that the person was, in fact, using a foreign device on the telephone line.

MR. FELDMAN: And was Agent Simon the FBI agent who was assigned to these investigations?

MR. BELLER: Yes, he was.

MR. FELDMAN: Agent Simon, how many cases ultimately resulted from the information provided to you?

MR. SIMON: The resulting investigative cases? We had five cases that were brought to indictment and subsequent prosecution. We had seven other cases that, because of the United States Attorney's position, prosecution was declined. And I will give you one specific example, where an individual made a blue box which was very unsophisticated in comparison to what Mr. Caming showed us. This blue box was approximately two-and-a-half feet long by two feet wide and about 18 inches tall.

This man made it at home from various electronic parts, and his wife used this device to call her mother once a week in Miami, Florida.

You have to understand, of course, that we did conduct extensive investigation to obtain all the facts we could before we presented them to the United States Attorney.

There were other telephone numbers referred to me by Mr. Beller where we subsequently obtained affidavits in support of a search warrant and subsequent search warrant were executed and we had what is known as a "dry hole." The device was not there.

As we progressed with these investigations we became more sophisticated. We learned with each one.

MR. FELDMAN: If we could concentrate on the five successful investigations, I believe that information came to you as to the FBI from a number of different sources, indicating that various defendants were using electronic toll-fraud devices. I wonder if you can state the different ways in which this information came to your attention.

MR. SIMON: There were three different ways. Mr. Beller would furnish us with a computer tape

printout, and after the issuance of a federal grand jury subpoena directed to Mr. Beller or his designee, he would furnish us with the name and address of the individual.

We would then conduct a physical surveillance to determine if that person actually existed. It is also possible to have aliases. We did run into a number of instances where an individual who was subscribing to the telephone company service was not, in fact, the name that was on that card.

So once we established this, and after obtaining a search warrant, we would notify Mr. Beller.

Mr. Beller, in turn, would notify one of his technicians who would tell us that there was, in fact, a device being utilized on that telephone.

MR. FELDMAN: Excuse me. I want to get into that but I want to initially begin by getting on the record the way in which the information initially came, not what you did after you received that information, but the various ways the information came to your attention.

MR. SIMON: I see. By Mr. Beller to our office—Mr. Beller's information.

The second thing we had was confidential source information.

MR. FELDMAN: And these were FBI informants who provided you information just as in any other criminal activity?

MR. SIMON: I'm sorry, Mr. Feldman. I didn't understand that.

MR. FELDMAN: These were FBI informants who would provide you with information that electronic toll fraud was occurring just the same as they'd advise you of gambling offenses?

MR. SIMON: That is right. And Mr. Moore was first brought to our attention by a confidential source who furnished the information to an agent of the FBI, Mr. J. Lawrence Sullivan. Mr. Moore did not have any of these devices even though he was selling them in Las Vegas. We were able to pick up Michael Raymond Tullis who was subsequently tried and convicted for fraud by wire, based on the confidential source information.

MR. FELDMAN: So you have computer printout information and informant information. Was there any other?

MR. SIMON: Yes. On Frank Joseph Masterana—he had been the subject of a number of legal Title III wire interceptions by not only the Las Vegas Division but other Divisions of the FBI. He was at one time in Macon, Georgia, for sentencing on one of the gambling cases, at which time confidential source information was received that he was using, in Macon, Georgia, at that time, a blue box to call Las Vegas.

So bearing this in mind and having additional information, two of our Las Vegas FBI agents, in August of '73, observed Masterana in an open pay telephone booth making a telephone call with what appeared to be a blue box. But they couldn't get close enough because he was quite surveillance-conscious.

Based upon that and subsequent investigations, we were able to assume that he was using a blue box, but we couldn't put it all together factually.

In conjunction with advice furnished by Strike Force Attorney James Duff, who is assigned to the Las Vegas, California, Strike Force Office, we, together with the telephone company, worked out a program whereby if we were able to come up with the various telephones that Masterana was using to make these alleged calls, Mr. Duff would give us authority to make an immediate arrest, providing the telephone company could verify the fact that Masterana was using an electronic device or a blue box.

MR. FELDMAN: These were all pay telephones?

MR. SIMON: Pay telephones. I hope I made myself clear at the beginning. These were pay telephone booths. What was required was to send agents out in the field and survey Masterana on a continuous basis to find out what telephone exchanges he was using.

After several days' work, we were able to determine he was using three or four different exchanges.

MR. FELDMAN: You determined the telephone booth he was using on a regular basis?

MR. SIMON: Yes. And incidentally, he was very careful. He would use an open pay phone in a drug store, for example, that was inside of the drug store, where he could view the exterior entrances into the drug store, watching for agents. And because of the size of the city of Las Vegas, it didn't take him very long to find out who we were. So it was difficult to surveil him.

MR. HODSON: Would you spell the man's name?

MR. SIMON: M-a-s-t-e-r-a-n-a.

May I continue?

MR. FELDMAN: Let me ask Mr. Beller a question.

Mr. Beller, Agent Simon has indicated now that not only was information secured initially from you, but information also came directly to him. Is it true that in cases where Agent Simon received information, he would then make that information available to you?

MR. BELLER: Yes. He would ask us to more or less verify the fact that this person was or was not using a blue box.

MR. FELDMAN: Would you explain to the Commission what method and equipment you used to make that verification?

MR. BELLER: Initially—and this is going back to the inception of when we became aware of the blue box—we had the computer printout. In addition, we had a brush recorder which would emit irregular type signals if, in fact, a person was using a foreign device on the line.

Subsequently, we acquired—the proper name is a northeast electronic dialed number recorder, Model No. TTS-176—which indicates the date, the time, and the number called. And it produces a tape such as this (indicating).

MR. FELDMAN: That is the tape produced by it?

MR. BELLER: Yes. Now, on the tape it more or less will show when, in fact, a person is using a foreign device, because it emits an irregular type of signal on here.

MR. FELDMAN: Was the signal on the tape?

MR. BELLER: It is more or less a percentage mark, and then it shows the person is emitting a key pulse which is other than what is normally emitted from a telephone.

MR. FELDMAN: Basically, that tape reflects in a physical fashion the action that Mr. Caming described earlier when a blue box is used, the various kinds of tones which must be punched in order to gain access to the line.

MR. BELLER: Yes.

MR. FELDMAN: That is produced in a visual fashion?

MR. BELLER: Yes.

MR. FELDMAN: Does that unit continue to reflect every call subsequently made over that line?

MR. BELLER: Yes, it does. It reflects local and long-distance calls.

MR. FELDMAN: Whether or not the call is completed?

MR. BELLER: That is right.

MR. FELDMAN: So with the use of this piece of equipment, once it is connected to the suspect line, you then have a complete record of every signal that has come across that line?

MR. BELLER: That is correct.

MR. FELDMAN: And in your experience, is the TTS-176 accurate in determining if these blue box signals have occurred?

MR. BELLER: Yes. We have no reason to believe it is not 100 per cent accurate.

MR. FELDMAN: Has this material been introduced in court?

MR. BELLER: Yes, it has.

MR. FELDMAN: And it has been accepted as evidence there?

MR. BELLER: I believe that is correct, yes.

MR. FELDMAN: At the time you hooked the piece of equipment on to the suspect lines—and this occurred on at least five different occasions, in five separate investigations—at that time were you aware that Section 2511(2)(a)(i) includes a rather broad provision allowing telephone companies to engage in voice monitoring?

MR. BELLER: Yes, I was.

MR. FELDMAN: In situations such as this?

MR. BELLER: Yes.

MR. FELDMAN: And with that knowledge you decided to conduct your investigation without actually engaging in voice monitoring?

MR. BELLER: That is correct.

MR. FELDMAN: Mr. Berolzheimer, were you involved in the decision-making process to come to that decision?

MR. BEROLZHEIMER: Yes, I was.

MR. FELDMAN: I wonder if you could just describe for the Commission the elements that went into it.

MR. BEROLZHEIMER: Well, essentially, we have had some experience in the Centel System which led us to take a very conservative position with respect to voice recording. And it has been our policy in that system for approximately ten years not to engage in any voice recording. We recognize the language of Section 2511(a)(2), and as I indicated in our statement, I believe the authority contained in that statute should be there. I can conceive of circumstances where it would be necessary to engage in voice recording to effectively secure convictions.

We did not believe that the situations as they existed warranted that. As a matter of fact, after the initial directives were given to Mr. Beller in 1973, the issue had never been raised again. The investigations were conducted. The evidence was accepted in court and convictions were obtained and we have really not faced that issue again.

MR. FELDMAN: Who participated in the decision-making process in these particular instances besides yourself and Mr. Beller?

MR. BEROLZHEIMER: Attached to the report which I furnished to the Commission was a letter from John R. Thompson to Mr. Beller—if you will excuse me a moment I'll find that letter. It is a letter dated April 26, 1973, to Mr. Beller from John R. Thompson, whose title is Senior Attorney. He is Senior Attorney with Central Utilities and Telephone Corporation, which is the parent company (Central Telephone Company).

You will notice also in that letter there are carbon copies addressed to Messrs. Garnett, Laggett, and Geary. Mr. Garnett is the Executive Vice President of Central Telephone and Utilities Corpora-

tion, Mr. Laggett is the Vice President for Telephone Operations, and Mr. Geary was at that time the Division Manager of Central Telephone Company in Las Vegas.

All of us participated in that decision, as well as, I might say, my partner, Melvin A. Hardies, and my partner Duane A. Feurer, all of whom worked on the matter from a legal standpoint.

MR. FELDMAN: Was a representative of the Los Angeles Strike Force involved in this also?

MR. BEROLZHEIMER: In no way. It was an internal decision.

MR. FELDMAN: And so no representative of the FBI or other agents were involved in that decision?

MR. BEROLZHEIMER: No, sir. The question was raised by Mr. Beller when he received the request, and we responded with this letter.

Also, substantially contemporaneously, a directive was prepared and issued along the same lines.

But that was strictly an internal policy decision. It was not discussed with any other outside organization.

MR. FELDMAN: Fine.

Mr. Beller, once you had verified to your own satisfaction, using the electronic equipment, that, in fact, electronic toll fraud was committed on these lines, what did you do?

MR. BELLER: Concurrent with the subpoena from the FBI, we'd typically put on the recorder to that particular individual's line. At that point in time, Mr. Simon would hand-carry over a subpoena for any and all information that we would have relating to toll fraud.

MR. FELDMAN: What type of information specifically?

MR. BELLER: Well, he would ask for the subscriber information card which denotes the name of the particular person who has the line, any other information that we might have, which would then be the paper tape.

MR. FELDMAN: The paper tape?

MR. BELLER: That is correct.

MR. FELDMAN: Agent Simon, I wonder if you could indicate what your next step was once you had received the information Mr. Beller had described?

MR. SIMON: Once we received the information, again our investigative process was to verify the fact and physically observe the home or apartment to see that we had everything correct, and based upon that information I would take the information furnished by Mr. Beller on the one 800 number, the toll-free number, and I would call it that day or the next day to verify the fact that it was a toll-free

number to a particular place. In some instances that number was no longer actually working, but the person utilizing the blue box could get into the toll-free telephone line system and use that number to get into it.

Then I would take that information and prepare an affidavit in support of a search warrant. This affidavit was then brought before the U.S. Magistrate who reviewed it, and through the normal process a search warrant was issued.

Then I would return to my office and contact Mr. Beller and tell him we had a search warrant at that time.

Then the next step was that whomever Mr. Beller would designate—one of their electronic experts—would call me and say they had information at this particular time an electronic device was being used on this telephone.

MR. FELDMAN: Was that information gathered by continued use of the TTS-176?

MR. BELLER: Yes.

MR. SIMON: This may have taken two days to prepare. Then there would be agents in the field and I'd notify them by radio. They had the search warrant, plus inventories in their possession, and they'd go in the house with a lawful search warrant and execute it.

MR. FELDMAN: And this was the same general procedure you used in each of the cases?

MR. SIMON: With the exception of the Masterana case.

MR. FELDMAN: And what occurred in that case?

MR. SIMON: In the Masterana case the Central Telephone Company was able to put on the device after we had surveyed the phones he had used. If we could tell what exchange Masterana was using, the telephone company would put on their TTS-176 and be able within ten minutes to tell us whether he was using an electronic device, the possession of which was not in violation of the law so he had to be using it. And as a result, we arrested Masterana in a telephone booth specifically on October 15, 1973, in a public pay telephone booth, at which time he had two blue boxes in his possession, the one he was using, together with voluminous gambling records, and \$18,836.53 was confiscated.

MR. FELDMAN: In the other four cases, when you executed the search warrant, who did you find in the premises and did you find a blue box in each case?

MR. SIMON: Yes, in each case. In the Judith Dinah Douglas case, two blue boxes were found when the search warrant was executed. As a result of this, she, Douglas, was tried by stipulation of facts and found guilty. She was sentenced to serve

five years in custody of the Attorney General of the United States on July 2, 1974, provided she'd submit to psychiatric examination, and come back within 90 days for resentencing.

Subsequently, her case was appealed to the Ninth Circuit on two separate occasions. The Ninth Circuit upheld the conviction. She has not to my knowledge begun serving her sentence, nor is she through with her legal recourse. Apparently she is going to appeal again.

On the Michael Raymond Tullis case, upon execution of the search warrants based upon confidential source information, we did find one device in his apartment, and this case went to jury trial.

He subsequently appeared on March 15, 1974, with counsel in Las Vegas and was sentenced to five years in custody of the Attorney General, with the first 90 days to be served in custody, and the balance of the sentence was suspended and he was placed on probation for the additional period.

In the Frank Victor Scaramuzzo case, with a valid search warrant we recovered a blue box and went to trial. He was found guilty on March 28, 1974, by the jury. On May 10, 1974, the United States District Judge in Las Vegas suspended his sentence and placed him on three years' probation.

At this time he also ordered that Moore make restitution to the Central Telephone Company.

He filed a notice of appeal to the Ninth Circuit and the Ninth Circuit upheld the conviction.

MR. FELDMAN: Agent Simon, are you aware of the thrust of that appellate court decision?

MR. SIMON: No, I am not. Mr. Stuart Rudnick, the strike force attorney who handled these cases, has that.

MR. FELDMAN: I believe Mr. Berolzheimer has a copy of the decision.

MR. BEROLZHEIMER: I do.

MR. FELDMAN: Are you familiar with it?

MR. BEROLZHEIMER: I have read it.

MR. FELDMAN: Was the basic thrust of it on the sufficiency of the search warrant?

MR. BEROLZHEIMER: No, I don't believe it was. The thrust of the decision was basically whether Section 1343 prohibited fraud by wire against a third party, or also covered fraud by wire against the carrier. And the court held it did cover fraud by wire against the carrier.

MR. FELDMAN: That is the Scaramuzzo case?

MR. BEROLZHEIMER: That is the Scaramuzzo case.

MR. FELDMAN: Do you also have the Douglas case?

MR. BEROLZHEIMER: I also have the Douglas case.

MR. FELDMAN: Does the Douglas case also deal with the sufficiency of the search warrant?

MR. BEROLZHEIMER: The Scaramuzzo case is reported at 505 Fed.(2d) 102. The Douglas case is reported at 501 Fed.(2d) 266.

The Douglas case does, as you indicate, turn essentially upon the validity of the search warrant.

I might note that the court indicated that three of the issues raised in the Douglas case had just recently been decided in the Scaramuzzo case and they were conceded except with respect to further appeals.

But in the Douglas case, the court did refer to Agent Simon's affidavit and the validity of the search warrant which was obtained based upon the methodology which Mr. Beller and Mr. Simon have just described, and did uphold the validity of the search warrant based upon that methodology.

MR. FELDMAN: Thank you.

Agent Simon, do you want to quickly continue with the results of these investigations so we can get those on the record?

MR. SIMON: Yes.

The last matter—I believe I have indicated the sentencing of Masterana.

The last matter was David Louis Goldberg and H. Jordan Rabstein. In this particular matter, in the fall of 1973, we had a court-authorized wire interception on Mr. Goldberg's residence phones. During that period of time, while we were monitoring and recording, we found on a repetitive basis that Rabstein would attempt to use the blue box or the electronic device to circumvent the telephone toll call recording equipment. It was a sophisticated type of blue box, slightly larger than the one Mr. Caming presented.

We heard him on numerous occasions make mistakes and because of the slowness with which he had to manipulate the call numbers, it apparently would not work successfully. Once in awhile he'd complete a call and be completely elated. Mr. Goldberg, on the other hand, was much more efficient.

Subsequently, Mr. Beller came to us with computer tape printouts, and we went through our normal process of obtaining an affidavit in support of a search warrant and subsequently a search warrant and executing the same, at which time we found one blue box in his residence, next to his night stand, which he had access to—his wife would, too, but he was the one who normally used it. And also we were able to seize three illegal, unregistered sidearms that he had in the apartment.

Mr. Goldberg, subsequently, together with Mr. Rabstein and with counsel, were charged with violation of the Title 18, Sections 1084 and 1343 of the United States Code. And they appeared and entered a plea of guilty.

They were subsequently sentenced on August 18, 1974, at which time Goldberg was sentenced to one year in custody of the Attorney General of the United States for violation of Section 1343, and Goldberg was placed on one year probation for violation of Title 18, Section 1084, both sentences to run consecutively.

MR. FELDMAN: Agent Simon, you have already indicated that Section 1343 does not specifically prohibit the possession of blue boxes.

MR. SIMON: To my knowledge, the manufacture or possession.

MR. FELDMAN: And in all cases, except the Masterana case, I assume, you arrived there sometime after the call had been concluded?

MR. SIMON: It was circumstantial.

MR. FELDMAN: That is my point. The evidence on which convictions were subsequently obtained was circumstantial.

MR. SIMON: That is right.

MR. FELDMAN: Were you involved in the post-arrest investigation?

MR. SIMON: Yes.

MR. FELDMAN: I wonder if you can describe the type of circumstantial evidence that was used in these cases?

MR. SIMON: We had the computer printout and the TTS-176 tapes—not only that was previously given to us but of that day, of the time, the Central Telephone Company had the TTS-176 installed on that phone or particular phones. That became part of the evidence we presented. Plus the fact that these people were the only ones in the apartment when the search warrant was executed helped us, of course.

In one instance, in the Scaramuzzo case, he called his attorney in the presence of Special Agent John Kinsinger—and I am going to paraphrase what Scaramuzzo said. He said, "They caught me with one of them things," or, "They caught me with one of them boxes and I was using it."

What he was saying is he had just set it down when the agents entered the room. And he set it down to answer the door and the phone was off the hook. We were able to introduce this and it was very strong.

MR. FELDMAN: And that was the basis on which convictions were obtained?

MR. SIMON: That is correct.

MR. FELDMAN: Thank you.

I have no further questions, Mr. Chairman.

MR. HODSON: I'd just like to clarify in my own mind what we have here.

The computer printout—do you have someone who examines those every month? How do you locate the person that you suspect?

MR. BELLER: Well, these come out regularly on all toll numbers. And, yes, we do have an individual who does examine them periodically to see whether or not there are any prolonged periods of calls on the toll-free network.

MR. HODSON: So that is just a visual examination that you go through?

MR. BELLER: That is correct.

MR. HODSON: It is not absolutely clear to me, but I assume there was no voice overheard at all in any of the cases?

MR. BELLER: That is correct.

MR. SIMON: Absolutely not.

MR. HODSON: And Mr. Berolzheimer, you indicated in your opening statement that you agree with Mr. Caming that there would be cases in which you would have to have voice overheard.

MR. BEROLZHEIMER: That is right.

MR. HODSON: And I wondered, in view of the foolproof method of solving a case that you were talking about, when you said there were certain cases where you must have voices overheard . . .

MR. BEROLZHEIMER: I want to make clear that Central Telephone Company, although it operates in nine states, has only had experience with this problem in Las Vegas. We only have experience in one area. You will notice from the material we have submitted to the Commission it all occurred during a relatively short period of time in 1973. It deals with one community, Las Vegas, which has relatively compact and flat geography with wide streets and low buildings.

It also happens to be the center of legalized gambling which also attracts a certain amount of illegal gambling and transmission of gambling information.

So we have in Las Vegas a combination of unique circumstances, including its geography, its size, the interest of both the FBI and the prosecuting agency; I think also the existence of a grand jury and the ability of the FBI to obtain search warrants.

We also had cooperation between the telephone company and the FBI, as has been described by the witnesses, with surveillance and radio control, so that they could swoop in and get the blue box.

I don't know, because we don't have the experience, but I certainly can conceive it would be most difficult to obtain that kind of evidence in a major metropolitan area. I just don't think you could coordinate it that well. Your ease of movement wouldn't be the same. Your distances would be greater; you'd have different kinds of courts.

And I am not convinced, although we were successful—that is, the U.S. attorney in Las Vegas was successful—in securing convictions in these six cases, without positive identification of the user, I

don't know that evidence would be convincing in every court. It had not become a critical issue in the cases tried in Las Vegas, but I can conceive of a court taking the position that without voice evidence of the user a conviction could not be obtained.

MR. HODSON: Mr. Caming, I wonder if you'd join the testimony.

MR. WESTIN: As to those comments which were made about the difficulty of investigation and confirmation, you seemed to be in agreement. I wonder if you'd say a word or two about that since you are directly involved in the investigative procedure. Do you believe these techniques would not be feasible in a large metropolitan center or under conditions that vary from the Las Vegas one?

MR. SIMON: I think all of the statements were very valid. Because of the fact that I spent ten years in Chicago, I can only express an opinion, but I can't conceive of this working in an apartment complex, a high-rise, third-floor walk-up. I think it would be almost impossible. If the technology was available, we might be able to proceed, but I don't think we could enter the residence within from one to five minutes after the telephone company says, "The electronic device is being used right now by an unknown party in Apartment No. so and so."

I think it would be almost impossible to have the physical surveillance work because of the largeness of the metropolitan area. I think it would be almost impossible to surmount. I just don't know how it could be done.

MR. WESTIN: Yet, on the other hand, if you imagine the array of evidence being presented to a jury that is being described, in which you have the computer printout, you have the brush tape, you have whatever extra time it might take until you get there, you physically find the blue box there—I am not sure why the case would collapse at that point.

MR. SIMON: My experience has only been in Las Vegas, but I am suggesting that in a large metropolitan area it possibly would not work as efficiently.

As an example, in the Michael Raymond Tullis case, our agents were delayed by a few minutes before they were able to execute the search warrant. Michael Raymond Tullis told us—told the agents who executed the search warrant—that approximately two minutes before they entered there were three other men in his apartment.

Now, our agents did not seem to believe him, for reasons unknown to me, but nevertheless, I could conceive of the Tullis case where you did enter that apartment and there were several people there. The identity of the person who used that electronic device may be up in the air, and it may be hard to convince the jury, possibly.

MR. WESTIN: Thank you.

MR. HODSON: I want to ask Mr. Caming a question in the same area. But before that, is it your view you have to find the man with the blue box and the phone off the hook?

MR. SIMON: I'm sorry. I didn't mean to give that impression. I think we have to have a strong circumstantial evidence case, as we did where we could come up with a TTS-176 tape, and have the cooperation of the telephone company to say an electronic device is being utilized at this moment at this phone, and have the agents have accessibility to the residence. The phone does not have to be being used.

MR. HODSON: The blue box has to be pretty warm.

MR. SIMON: Not only that, but in the Judy Douglas case, the FBI Laboratory in Washington found two of her fingerprints on one blue box, so that helped us considerably.

MR. HODSON: Mr. Caming, you have heard the testimony these gentlemen have given about these five cases. In your testimony, you indicated you get a short period of voice overhearing. Would you explain why you feel this is necessary?

Secondly, does Bell also use the system we have just heard about?

MR. CAMING: First, I might like to say, Mr. Hodson, I am in general agreement with everything said by Mr. Simon and the gentlemen from Central Telephone. In fact, we agree completely. And we have found in a number of cases where we, too, have been fortunate because of proximity and circumstances in the thousand or so cases we have been involved in in the last decade, if we could catch them using it or in circumstances very close to that, as Mr. Simon so ably described in one or two of the cases, then we either could obtain a plea of guilty or they would be found guilty.

But we have found in the majority of our cases, and those that are the greatest problem to the industry as a whole, that we have not been able to have such a happy admixture of factual circumstances. And let me give you three cases just as an example of what we have been through.

Problems of identification have been very great. We had one recently that we received invaluable help from law enforcement authorities on. And I might generally say that over the years in many areas, not only electronic fraud, the cooperation of the Bureau has been consistently outstanding. And I think it is worthy to express what is a personal feeling but a tribute to their industry and dedication.

As far as this one case, it is a case that might be denominated—the Bremson case—only because he

was one of the original architects. Since time is of the essence, I will quickly synopsis it. It involved the general cooperation of 14 Bell Telephone companies and two General Telephone companies, between December 1971 and September of 1972.

I will just name the cities that were principal cities: Minneapolis, Cleveland, Houston, Dallas, Los Angeles, Santa Monica, Atlanta, Washington, D.C., Chicago, Detroit, Des Moines, Memphis, St. Paul, Miami, New York, Denver, Knoxville, New Orleans, Milwaukee—among others.

We finally resulted in gathering evidence—as you can see, this was a very widespread conspiracy of manufacturers, nationwide distributors, and users, such as businessmen. The purpose was to not only very substantially manufacture and distribute blue boxes, but to use them in an extensive number of businesses where you might have offices populated by a large number of people, and where it was virtually impossible to maintain surveillance of any intimate character.

Also, these people used them at homes scattered throughout a large area.

It finally resulted in 20 arrests, 19 indictments, at least 14 convictions—a number of investigations are still going on.

In another case, to show you how cogent the problem is, financier Bernard Kornfeld was involved. He apparently had a home which I understand was huge, something like 90-odd rooms, in the California area. There was a large number of people, both male and female, constantly in and out of there. There were indications from various sources of some use by somebody of blue boxes in some parts of this rather cavernous place.

Finally, it resulted in apprehension by chance of one of the secretaries using the blue box, and she was arrested on January 28 of 1975. The question of identification was critical and could not have been made except for the very limited voice recording.

It ultimately resulted in the seizure of two boxes. And even with all that, it took six months more to develop the case, to indict Mr. Kornfeld on June 5, 1975, by a federal grand jury in Los Angeles, some six months later, for making 344 calls to Europe over a period of time.

These are just several cases. A third was *United States v. Damato* in the Eastern District of Pennsylvania, which involved interstate gambling. Black boxes were involved as well as the so-called cheese boxes. This required the cooperation of a large number of companies and very coordinated activity.

None of this information could have been obtained as far as identifying the individuals, deter-

mining the extent of the conspiracy, and when the calls were completed or whether they were personal calls or part of the conspiracy, without this minimal amount of recording. This was in addition to the other aspect.

It has been our experience that where we can obtain the box, and it is a relatively simple case as far as factual circumstances permitting concentrated activity, we could probably make the case. But in the majority of the cases, it has been our experience that some voice recording was necessary.

MR. HODSON: In summary, the slight amount of voice recording is necessary for identification of the person using the phone?

MR. CAMING: Exactly. And I might point out that in all cases that have been subjected to judicial scrutiny, the courts pointed to this with approval. And the voice recording usually is limited to a few calls, also. In other words, we don't sit normally on a telephone to build up a record.

There is another point. It is virtually impossible to avoid some voice recording in a widespread conspiracy like the Bremson case—or there is one that just occurred in Montana, in the northwestern part, that stretched throughout the northwestern part of the United States.

And there was another one recently between Portland and Arizona, sales and manufacture.

MR. HODSON: You mentioned several times a conspiracy case. Are you referring only to conspiracy to defraud the telephone company?

MR. CAMING: Yes.

MR. HODSON: Or are you talking about conspiracy to murder?

MR. CAMING: No. I might point out none of our evidence—gathering at any time is in any sense for any crime except the theft of toll service. It is only the opening salutation that is recorded. And the only purpose we use it for is for that purpose.

MR. HODSON: I am satisfied with your answer.

May I ask this of Mr. Beller.

Would your means of following the toll fraud work in the case of a black box which, as I understand, is a box used by the receiver of a phone call?

MR. BELLER: We have never had any experience with the black box in Las Vegas.

MR. HODSON: In your experience, Mr. Caming, would it work on the black box?

MR. CAMING: It would be more difficult to work with a black box. Of course, if you could find a black box in use and caught the person in the act, of course, it might well be sufficient circumstantial evidence. We find it very difficult with black boxes.

MR. HODSON: You would not have the computer printout to start with, would you?

MR. BELLER: No, that is correct.

MR. HODSON: So you would have to do it another way completely?

MR. WESTIN: I understand our three witnesses have to leave. We very much appreciate your coming and giving this testimony to us. Is there anything else you'd like to add?

MR. BEROLZHEIMER: I'd like to add a couple of quick points. When Agent Simon was testifying, he said there were three methods for obtaining information about blue box cases, and he actually mentioned a fourth, and that is the Title III wiretap they were using in the case where they overheard. Second, while Central had this period of activity in 1973, despite the fact it has continued to use the computer printout and other indications of use, it has not developed evidence since then. It is not known why. It may be the fact there have been six convictions, and those convictions have had a prophylactic effect. We don't know why, but we know we haven't had any successful activity in finding any since late 1973.

Third, I would like to point out one of the areas of the law that is uncertain in Section 605 of the Communications Act. This issue came up in a conversation that we had last week with Mr. Rudnick in Las Vegas, the question of demand of lawful authority. And I indicated to him that as far as I was concerned, that didn't mean anything to me, that I didn't know what demand of lawful authority meant in the statute, and as long as I was attorney for the company I would not authorize disclosure except in response to a subpoena or court order because I don't know what that clause in the Communications Act means, and perhaps the Commission should address itself to that question.

And finally, despite the fact I agree with Mr. Caming that there are circumstances where a voice recording will be necessary, so long as I am advising Central Telephone Company, I know I am going to be very reluctant to authorize voice recording except when we are presented with a situation such as the conspiracy that he referred to, because the company does feel that its primary obligation is to preserve the privacy of communication.

Thank you very much.

MR. HODSON: Mr. Chairman.

MR. WESTIN: Yes.

MR. HODSON: You have raised a question by mentioning Title III. It seems to me you have enough evidence as you go down the line to get a Title III order to overhear in order to solve the toll fraud. I'd like to have your comment, Mr. Berolzheimer, and also yours, Mr. Caming, on that. It seems to me you have enough evidence to establish probable cause.

MR. BEROLZHEIMER: I don't believe you could get a Title III order for the purpose of finding a Section 1343 violation.

MR. FELDMAN: I was going to raise this: The detection of blue boxes and black boxes is not necessarily a recording versus nonrecording situation. The Commission is interested because of the broad scope of Section 2511(2)(a) which gives the telephone company greater leeway than anyone on this. There are no restrictions on their ability to monitor for toll fraud. The issue isn't recording versus nonrecording.

The other option might be to place 1343 under the list of proscribed activities for which wiretapping could be used and have the telephone company present that to the FBI after gathering information, and then allow the FBI to go in and seek a Title III court order.

Now, we discussed this with Mr. Caming before, and I am sure he is going to have some comments on it.

MR. CAMING: They might comment first if they have a plane to catch.

MR. BEROLZHEIMER: Let me just make a brief comment on that, and it is not a subject to which I have given a lot of attention. I am sure Mr. Caming is much more prepared to address it than I am.

Mr. Feldman raised this question with me the other day, and I told him and I do believe there is a significant distinction between the activities of the telephone company, which is a private party, taking action to protect itself against fraud being perpetrated on it—there is a distinction between that and government action.

And I think that that is really the essential distinction. And in our society, one of the things we are more concerned about is government action. And as long as the law enforcement officials and federal agencies are not involved in it, I think we have a different situation with respect to the carrier which is simply acting in its own behalf to protect itself.

MR. WESTIN: I understand the difference between the governmental and private sectors, but I think the carrier is being charged with a common carrier function, and given the important media of communication, a line could be drawn. It is a public function, publicly charged.

Why would your argument lead you to the conclusion against the court-ordered amendment to Title III that would say if you make out the evidentiary basis you gentlemen have described, the proper step would be to turn it over to the public authorities and have them do the recording, voice recording, as the final stage in the process of public prosecution. In that case, you protect the privacy of the telephone medium to its greatest.

MR. BEROLZHEIMER: I don't want to get involved in a long debate about it because I have not thought about it long or thoroughly, as I indicated. But I think the point you made is one of the essential points, that the carriers are regulated public utilities and subject to the regulations of the various states that have jurisdiction over them.

Second, I think the record shows the carriers have considered very seriously their obligation to protect the privacy of communication. Mr. Caming emphasized that in his statement, and I emphasized it in mine, and I think the history of this country bears that out, that the communications carriers have viewed their role very seriously and have given primary importance to their obligation to their customers to safeguard the privacy of communication. The law enforcement officials do not have that same responsibility or obligation. They look at it from a different angle. I think that is a critical difference.

MR. WESTIN: Again, let me thank the three of you for coming and testifying.

[The prepared statement of Mr. Berolzheimier follows.]

STATEMENT OF
KARL BEROLZHEIMER, ON BEHALF OF
CENTRAL TELEPHONE & UTILITIES CORPORATION

My name is Karl Berolzheimier. I am a partner in Ross, Hardies, O'Keefe, Babcock & Parsons, Chicago, Illinois, which is general counsel for Central Telephone & Utilities Corporation and its subsidiaries which I shall refer to as the "Centel System." The Centel System provides telephone service to more than 1,244,000 telephones in nine states. It is not affiliated with any other telephone system and is a part of the independent telephone industry. The five largest exchanges served are Las Vegas, Nevada; Park Ridge-Des Plaines, Illinois; Tallahassee, Florida; Charlottesville, Virginia; and Hickory, North Carolina.

In response to a request from Mr. Hodsen dated April 18, 1975, I filed a report with the Commission, by letter dated May 16, 1975, on electronic toll fraud investigations in the Centel System. For more than ten years I have had primary responsibility for advising management of the Centel System with respect to matters of secrecy of communication.

The only significant activity involving electronic toll fraud in the Centel System occurred in Las Vegas, Nevada during 1973. Mr. Neil Beller, an attorney employed by Central Telephone Company in Las Vegas will testify about that activity. I am here to answer any questions relating to Centel System policy or positions relating to the matters being considered. I have read Mr. Caming's testimony and, if desired, can comment upon it.

The Centel System considers its role to be that of a communications carrier. It is not in the business of providing investigatory or law enforcement services. Its primary obligation is to carry messages and preserve the privacy of those messages. Any intrusion is viewed seriously and undertaken only after receipt of appropriate legal authority. We would prefer that there be no intrusion under any circumstances but that is not possible in view of the authority granted in Title III of The Omnibus Crime Control and Safe Streets Act of 1968, as amended. Moreover, the

Centel System companies are subject to electronic toll fraud and must in fairness to its subscribers and stockholders, take whatever action is prudent to protect its revenues. The authority contained in Section 2511(2) is essential for this purpose.

We believe Section 1343 of Title 18 is a necessary tool and we support adoption of Section 1344 proposed by the Bell System.

If the telephone companies are to be able to protect themselves from fraud, prosecutors must have an appropriate statutory scheme. Since Blue Boxes have no lawful purpose, manufacture, transportation and possession of such devices should be outlawed. It will often be difficult to prove the necessary elements under Section 1343 and the Centel System endorses the proposed Section 1344.

As our report to the Commission stated, and Mr. Beller will testify, there have been six convictions in Las Vegas. Central Telephone Company has not engaged in any voice recording and the convictions were obtained without use of voice recording to establish use or identity of the user. Mr. Caming has suggested that there is no alternative but to make a limited recording of each illegal call (p. 19). Although the Centel System has not advocated such a procedure, and its experience would not indicate such a need, we do not disagree with Mr. Caming. The Las Vegas area, the only one in which the Centel System has experience with blue box prosecutions, is unique for several reasons. The area is relatively flat; it is a compact; and movement is easy. With the exception of a few hotels and office buildings there are few tall buildings. Since it is the center of legalized gambling there is also an interest in policing illegal gambling activities which have involved use of blue boxes. There has been very close cooperation between the carrier, the investigative agency (FBI) and the prosecutor. These factors have permitted gathering evidence adequate to obtain convictions under Section 1343. However, this experience does not indicate that convictions could be obtained in other jurisdictions based on the same evidence. Nor does it indicate that the same evidence could be obtained under different circumstances. For example, it would be most difficult to prepare and execute search warrants in a large metropolitan area in the same manner as has been utilized in Las Vegas. The method used in Las Vegas would not be adequate to gain evidence of a multi-city conspiracy.

Accordingly, the Centel System agrees that, under some circumstances, limited recording may be the only effective method of gathering evidence of an illegal call sufficient to secure a conviction.

Thank you for the opportunity to present this brief statement.

MR. WESTIN: Mr. Caming, would you give us your view on the issue and let us know how you perceive the issue?

MR. CAMING: May, I, before we advert to this subject, say one subject came up that you, Mr. Westin, might like to refer to with respect to amendments to Title III.

Section 605 as presently written, as amended in 1968—the first sentence really may be grammatically incorrect. You know, one court has interpreted it with respect to the intent. But it would seem to me that it does require rewording of the first sentence.

If you read it literally, it states that, "No person receiving or transmitting a communication shall divulge or publish the communication except

through authorized channels, (1) to any person other than the addressee," (2) —and then it goes on, 3, 4, and 5. So that literally it says you cannot disclose to any person in the telephone company, to the master of a ship, in response to a subpoena, etc. And I know one of the courts recently had to interpret this as saying, "Well, the literal language cannot prevail over the obvious intent of Congress."

And if you compare this with what was previously first clause of 605, you will see there is some change in punctuation.

I merely mention that because you had raised that question earlier.

MR. WESTIN: Actually, Section 605 is taken verbatim from a clause in the Radio Act, and it uses language that was appropriate for the transmission of radio communications. And when Congressman—the floor manager for that legislation—was asked what the floor debate on the legislation might be intending to change in the existing law, he replied, "Nothing," and I think he was well-borne-out despite the decisions of the Supreme Court, because anyone who sat down to draft a law for telephone communications couldn't have done worse than to take a law set up for radio.

So we are in third-generation fault here.

MR. CAMING: That is very true, and when they republished it in 1971—

MR. WESTIN: They didn't clean it up.

MR. CAMING: —they confused it further because it is more so than it was before '68.

To advert to your question—and I can understand the very legitimate concern of the Commission as to whether the court orders for toll-fraud monitoring in a carefully limited number of safeguarded cases would advance or be a deterrent to the public interest.

In our opinion, and in mine, it is definitely contrary to the public interest to require any more recording than is necessary. And the proposed method would, for reasons I will very briefly state, produce that adverse result.

First, we are not talking—as I mentioned in my statement—about wiretapping. That is, to obtain the content of the conversation of lawful calls, to obtain evidence of some crime other than the placing of the call. The only recording we do is with respect to calls that are illegally placed, and to prove the placing—not the content. We are not interested and we do not invade the content to obtain evidence of another crime.

Now, this is a very vital distinction in my opinion.

Secondly, we are acting in part pursuant to a statutory duty not only to prosecute but to bill. And for reasons mentioned in my statement, without

burdening you with the details set out therein, we have to bill and cannot allow free service to continue when we know it is being stolen.

The only recording we do is very limited, to identify not only the person but the actual completion of the call, so that you have a scintilla of probable cause that a crime was committed, and is actually being committed, because there is no lawful charges due until the call is completed, and to identify, to the extent of probable cause, that a certain person or persons committed the call.

So simultaneously with obtaining the very scintilla of evidence necessary to go to a court, you have all the recording and all the evidence necessary to prosecute.

If you went to court, we'd still have to do that little amount in order to have enough evidence to establish who committed the crime, and that a crime was committed, because even a John Doe warrant is no good without establishing that a crime was actually completed. And secondly, it is to establish if there is a conspiracy—and there is so often in these cases more than one involved—how it was done.

Now, when this evidence is presented in court, in almost 100 per cent of the cases where we get this evidence we prosecute. So that each case is subject to exhaustive judicial scrutiny, which is in the public interest, only on its very limited, carefully restricted recording under security conditions.

The contrast would be to turn it over to law enforcement after amendment of Title III to give them 30 days to monitor and record, which would only mean that you are going to have a much more extended period of recording.

MR. WESTIN: May I just ask you a question at that point. I am not sure I understand why that is the only alternative. Suppose the amendment said that on the production by you of the supporting documentations that have been described here, the computer printouts and brush tapes, and so forth, the law enforcement agent or even you could be directly authorized by the court—since I am not entirely convinced that we have to bring law enforcement in as the third party. I can see doing it either with or without law enforcement. But either way, the court would order identification of recording, not to exceed a reasonable time—a minute, 30 seconds, whatever. I don't see that automatically you have to go to 30 days. We could write a fresh amendment that would take your procedure, and the difference would be that in that case the disinterested party, the court, comes in, scrutinizes the proof that you have acquired, and because the procedure would then be done only with the authority of the court, something of the stain of the

telephone company doing it “by itself, unsupervised” might be withdrawn.

MR. CAMING: As I say, I can well understand the appeal of that. Unfortunately, we'd have to get sufficient recording to establish that the crime was completed and who did it. Otherwise, the courts would just be going on reasonably suspicious, rather than probable cause, on a John Doe basis.

MR. WESTIN: Let me ask you about that.

MR. CAMING: I'm sorry.

MR. WESTIN: Just precisely, if all the things were made out that we have heard here, wouldn't that be probable cause? You would know that from a given office or apartment there had been a device. The only question you would have, was it Mary Jones or Harry Smith or Jane Doe that was placing the call. As I understand the purpose of your voice recording, it is to identify an individual, not to make out the fact of the crime. All those things I assume you have done in what has been presented to us.

MR. CAMING: We haven't proffered proof that the call is completed.

MR. WESTIN: But you have shown the deviation from normal usage.

MR. CAMING: You have shown an attempt was made so far.

MR. WESTIN: If I assume everything just the way it has been described here today, and it is the identity of an individual for purposes of final proof and prosecution, what if we were to write an amendment or suggest to Congress that it write an amendment that would say at that point you would go before a judge, and the court would authorize the placing of an identification recording device on the phone. It would be done under properly supervised conditions, and at that point your case, then, is complete.

MR. CAMING: I would say that it has been our experience that there is no need for that. As I said, we are not wiretapping—just to mention that.

Secondly, there has been no abuse by the telephone industry and, if anything, our procedures have been further refined. We are talking only about calls that are unequivocally identified as illegally placed.

And every one of these in prosecution is completely scrutinized. The only purpose of gathering this evidence is for prosecution. And the courts have reviewed it and do review it, and you do have the judicial position. And in no case, with the possible exception of one, has there been any abuse.

MR. WESTIN: You appreciate that statement you have made is something you can make from your knowledge and belief. It is something that the public has to take, then, on faith, because there is

no public participation before the fact as opposed to after the fact when the court scrutinizes prosecutions that take place.

So what I am really raising with you is: How does the public—

MR. CAMING: Well, we are regulated. To give you an illustration, I recently have appeared on this very subject before the staff of the Common Carrier Bureau of the Federal Communications Commission. We are not a private party in the sense that we can act in an irresponsible fashion and very little surveillance. We have continual responsibility in every state and to the federal authorities through our regulatory commissions.

So you have that, plus the fact that the courts for ten years now—and it has gone up to the Supreme Court of the United States, and there has been no question in the mind of any court of any abuse or any impropriety.

To do the other—for example, if you did it with law enforcement being in the picture, it would mean that each case would not necessarily get the manpower, the attention, the expense we put in, because of the importance from a deterrent standpoint in the public interest of having a prosecution, to get this done properly.

And it would also—and I feel this is a point that I must say with delicacy—it would put us in the position of being hostage to law enforcement if they were engaged in this, as to the priority accorded to these cases and the amount of manpower and surveillance devoted thereto, and it might be said by those who are cynical—which, of course, I am not—that perhaps a quid pro quo might be asked for that might at times be disadvantageous to the public interest.

MR. WESTIN: That is why I can imagine a procedure that we might recommend and not bring law enforcement in as the third party but authorize the security office of the telephone company to do that voice recording.

Factually, I think it is true, and something that hasn't come out today, that in addition to gamblers using the black box devices, I think it has been shown to be the case that many student groups, New Left groups, et cetera, have published all kinds of, "Rip Off the Telephone Company" schematics and descriptions, and so forth, and there have been any number of anti-telephone company campaigns as part of political movements.

Therefore, the possibility that the telephone company could be used by law enforcement in the way that you were describing, for getting information about fugitives from justice and things like that, I would think can be thought to be quite real.

So I am quite sensitive to your point that law enforcement being brought in might open it up to the possibility of some other kind of abuse.

Therefore, I think some such procedure, as I have suggested, that leaving out law enforcement might be worthwhile.

MR. CAMING: Certainly, we would be responsive to any procedure that the Commission and Congress sees appropriate that would permit us with any proper accountability to maintain dominion over the evidence-gathering procedure. We think that is in the public interest. We are a public utility, regulated.

A great amount of time, effort, and expense must be devoted to these cases to do them properly—and we do them independently of law enforcement. This is very vital. As much as possible, we try to complete the package before them. So it can be said it is done independently. And the courts have commended us, as you probably know, in a number of cases for this conservative position.

I would say that certainly any method of legislation that would permit us to maintain dominion from one end to another over the process with such accountability as Congress finds desirable would be in the public interest, and therefore we would favor it.

MR. WESTIN: I think this exchange has been very helpful to us on the Commission in terms of exploring the needs that the telephone company sees and the protection of the resource and the issues that are involved in the public interest as well.

I know General Hodson has something he wants to ask you for the record.

MR. HODSON: Mr. Caming, recently I have been advised informally that the Senate Judiciary Committee, which is considering S. 1, the revision of the Federal Criminal Code, which would include 2510 and 2511 of Title 18, has amended 2511(2)(a)(i), the same section we have been talking about here, to eliminate all monitoring by the telephone company and by private industry, the owners of private switchboards—eliminate all monitoring except mechanical. That would eliminate service observing and supervisory monitoring.

I would like to draft a letter to you after this meeting, because time is short, and get your response to that proposal by the Senate Judiciary Committee, because I think it's a part of our report likewise, and I think we have to have something in the record on it. We would like to get your view. I will outline the broad areas in which I believe the Commission is interested, and with the approval of the chairman we will make that a part of the record.

[The requested material appears elsewhere in the record as a part of the staff study on service monitoring.]

MR. CAMING: Thank you for the opportunity. And should the Commission so desire, after receiving our response, we would be glad to appear before them; and in connection with our business subscribers as to that issue, you may wish to hear certain of them. I leave that to the discretion of the Commission. We'd be very pleased to respond.

MR. WESTIN: Thank you, Mr. Caming.

Mr. Feldman.

MR. FELDMAN: One feature might also include an inventory procedure. You are familiar with what I am speaking of? I gather that if at this time the telephone company engages in the limited recording which you have described but ultimately discovers they have not been able to determine the blue box is in use, the subscriber is never advised of the fact his conversations have been overheard; is that correct?

MR. CAMING: I would say that because of the methods we employ to determine, prior to any ultimate investigation of a voice recording characteristic, that in almost all of our cases when we go forward to the voice recording stage we prosecute it.

There is virtually no case I can think of where we would not be in a position to move in.

Now, ultimately the prosecutor may not wish to prosecute, but it is minimal, and in such cases we generally communicate directly with the offender. So I don't think that is a problem.

MR. FELDMAN: You have supplied the Commission with a draft statute which would prohibit the manufacture and sale, or importation and sale, of blue boxes and other electronic toll-fraud devices. The statute also proscribes the publishing of specifications, schematics, and instructions on the manufacture of such devices.

[The draft document referred to follows.]

PROPOSED FEDERAL STATUTE PROSCRIBING THE MANUFACTURE, DISTRIBUTION,
IMPORTATION, POSSESSION, ETC. OF DEVICES, OR SPECIFICATIONS THEREFOR,
FOR THE FRAUDULENT OBTAINING OF COMMUNICATION SERVICES

It is respectfully urged that a new section, § 1344, be added to Title 18, Crimes and Criminal Procedure, of the United States Code, to read as follows:

§ 1344. Fraudulent Communication Devices.

(a) Whoever willfully

- (1) sends through the mail, or sends or carries in interstate or foreign commerce, or
- (2) imports or otherwise brings into the United States or any territory or possession under its control or jurisdiction, or
- (3) makes, assembles or possesses, or
- (4) sells, gives or otherwise transfers to another, or
- (5) offers, or places in any newspaper, magazine, handbill or other publication any advertisement, to sell, give or otherwise transfer to another, or
- (6) purchases or in any other manner obtains, receives or conceals,

any electronic, mechanical or other device, instrument, apparatus or equipment, or plans, specifications, instructions or other information for making, assembling or using any such device, instrument, apparatus or other equipment, or publishing any such plans, specifications, instructions or other information,

with intent to use it, or knowing or having reason to know that it is intended to be used or that its design renders it primarily useful, to obtain any communication service from a communication common carrier,

by rearranging, tampering with, or making any unauthorized connection, whether physically, electronically, acoustically, inductively or otherwise to, any telephone instrument, equipment or facility of any such communication common carrier,

to avoid the payment, in whole or in part, of the lawful charge for such communication service, or to conceal from any such communication common carrier or from any lawful authority the existence or place of origin or termination of any communication,

or by using any communication service knowing or having reason to know that such rearrangement, tampering or connection existed at the time of use,

shall be fined not more than \$1,000 or imprisoned not more than five years, or both.

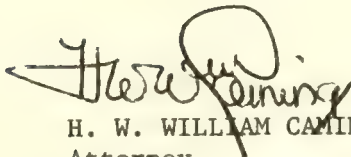
(b) As used in this section, "communication common carrier" shall have the same meaning which is given to the term "common carrier" in section 153(h) of title 47 of the United States Code.

(c) Any device, instrument, apparatus or equipment, or plans, specifications, instructions or other information therefor, described in subsection (a) of this section, may be seized and forfeited to the United States. All provisions of law relating to (1) the seizure, summary and judicial forfeiture, and condemnation of vessels, vehicles, merchandise and baggage for violations of the customs laws contained in title 19 of the United States Code, (2) the disposition of such vessels, vehicles, merchandise and baggage or the proceeds from the sale thereof, (3) the remission or mitigation of such forfeiture, (4) the compromise of claims, and (5) the award of compensation to informers in respect of such forfeitures, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this section, insofar as applicable and not inconsistent with the provisions of this section; except that such duties as are imposed upon the collector of customs or any other person with respect to the seizure and forfeiture of vessels, vehicles, merchandise and baggage under the provisions of the customs laws contained in title 19 of the United States Code shall be performed with respect to seizure and forfeiture

of any such device, instrument, apparatus or equipment, or plans, specifications, instructions or other information therefor, under this section by such officers, agents or other persons as may be authorized or designated for that purpose by the Attorney General.

(d) Nothing contained in this section shall create immunity from criminal prosecution under the laws of any State, the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States.

(e) If any clause, sentence, paragraph or part of this section or the application thereof to any person or circumstances shall, for any reason, be adjudged by a court of competent jurisdiction to be invalid, such judgment shall not affect, impair or invalidate the remainder of this section and the application thereof to other persons or circumstances, but shall be confined in its operation to the clause, sentence, paragraph or part thereof directly involved in the controversy in which such judgment shall have been rendered and to the person or circumstances involved.



H. W. WILLIAM CAMING
Attorney
American Telephone and
Telegraph Company
June 11, 1975

My final question is: Do you see any potential First Amendment problems with that part of the statute?

MR. CAMING: I really don't in the sense that there is no prior restraint. Actually, the publication of these plans and schematics is solely in association with these devices. It has no legitimate purpose whatever, and it makes the publication criminal but doesn't proscribe it. It just prohibits proceeding with impunity. And in that sense, I think it is within the general First Amendment constraints.

It is in effect designed only to the committing of what is patently an illegal act of an immediate character—the publication. In other words, the publication would result—

MR. FELDMAN: Your Act would make a criminal offense the publication of the specification?

MR. CAMING: Oh, yes. It is proposed to make criminal the publication of the schematics and diagrams.

MR. FELDMAN: And you don't feel there would be any First Amendment problem with that?

MR. CAMING: I think it is within the permissible limits of the First Amendment. I am sure that some may think that any limitation on speech, as one of our Supreme Court Justices said, is a First Amendment problem.

But I think the courts generally have said there are some limits beyond which you cannot proceed.

MR. FELDMAN: Thank you.

MR. WESTIN: It is very perilous to ask one last question and raise a First Amendment issue, so we will have to forego the joy of discussing the First Amendment limits with you.

Thank You very much, Mr. Caming.

MR. CAMING: Thank you.

MR. WESTIN: The Commission meeting is adjourned.

[Whereupon, at 6:20 p.m., the hearing was adjourned.]

BOSTON PUBLIC LIBRARY



3 9999 05705 8180

